ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

ANÁLISIS EN SEGURIDAD INFORMÁTICA BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001, PARA EL DISEÑO DE UN MODELO QUE PERMITA LA VERIFICACIÓN DE INTEGRIDAD DE DOCUMENTOS INFORMÁTICOS

MARILU DEL CISNE TORRES ROMERO

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de:

MAGÍSTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

Septiembre 2021

CERTIFICACIÓN:

El **Trabajo de titulación modalidad Proyecto de Investigación y Desarrollo:** titulado "ANÁLISIS EN SEGURIDAD INFORMÁTICA BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001, PARA EL DISEÑO DE UN MODELO QUE PERMITA LA VERIFICACIÓN DE INTEGRIDAD DE DOCUMENTOS INFORMÁTICOS", de responsabilidad de la Señorita: Marilú del Cisne Torres Romero, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Dr. Luis Eduardo Hidalgo Almeida; PhD
PRESIDENTE

Luis Eduardo Hidalgo Almeida
Firmado digitalmente porLuis Eduardo Hidalgo Almeida
DN: cn=Luis Eduardo Hidalgo Almeida gn=Luis Eduardo Hidalgo Almeida c=EC Ecuador l=EC Ecuador o=ESPOCH ou=Instiuto de Posgrado y Educacion continua e=l_hidalgo@espoch.edu.ec Motivo:Soy el autor de este documento Ubicación:
Fecha:2021-11-16 17:03-05:00

Ing. Cristian Merino Sánchez; MSc.
DIRECTOR

CRISTIAN GEOVANNY MERINO SANCHEZ
Firmado digitalmente por CRISTIAN GEOVANNY MERINO SANCHEZ
Fecha: 2021.11.15 13:32:31 -05'00'

Ing. Silvia Morales Noriega.; MSc.
MIEMBRO

SILVIA LORENA MORALES NORIEGA
Firmado digitalmente por SILVIA LORENA MORALES NORIEGA
Fecha: 2021.11.13 17:50:56 -05'00'

Ing. Paúl Xavier Paguay Soxo; MSc.
MIEMBRO

Firmado electrónicamente por:
PAUL XAVIER PAGUAY SOXO

Riobamba, septiembre 2021

DERECHOS INTELECTUALES

Yo, Marilú del Cisne Torres Romero, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

Firmado electrónicamente por:
MARILU DEL CISNE TORRES ROMERO

Marilú del Cisne Torres Romero

Nº de Cédula: 1104934375

DECLARACIÓN DE AUTENTICIDAD

Yo, Marilú del Cisne Torres Romero declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este Trabajo de Titulación de Maestría.

Firmado electrónicamente por:
MARILU DEL CISNE TORRES ROMERO

Marilú del Cisne Torres Romero

Nº de Cédula: 1104934375

DEDICATORIA

Este proyecto lo dedico principalmente a Dios por toda la fortaleza que me brindó siempre y por ser mi guía en todo este proceso.

A mis amados padres, Segundo y Gladis quienes con su amor, esfuerzo y paciencia siempre me brindan su apoyo y gracias a ello hoy logro cumplir una d mis metas

A mis queridos hermanos Robinson y Cristhian que durante toda mi vida han sido mi gran soporte y me han inspirado a seguir adelante.

A mis sobrinos y toda mi familia que con sus oraciones, consejos y palabras de aliento hicieron de mi una mejor persona y de una u otra forma me acompañan en todos mis momentos.

A mis buenos amigos; a mis queridos maestros, coordinadores y tutores que siempre compartieron conmigo sus conocimientos y me apoyaron en el transcurso de mis estudios de posgrado.

Marilú

AGRADECIMIENTO

Agradezco a Dios por brindarme día a día esa gran fortaleza y voluntad para no dejarme vencer en ningún momento, a mis padres y mis hermanos por su apoyo y amor incondicional quiero decirles que una vez más estoy cumpliendo esto que me propuse, gracias por estar conmigo siempre.

Mi profundo agradecimiento al "Instituto de Posgrado y Educación Continua" de la "Escuela Superior Politécnica de Chimborazo" y a todo el personal del mismo, a mis maestros de quienes recibí sus conocimientos y a mis buenos compañeros con quienes compartí gratos momentos. De manera especial, un agradecimiento a nuestro coordinador de maestría Ing. Oswaldo Martínez, a mi tutor de Tesis, Ing. Cristian Merino, y miembros de tribunal, agradezco su dedicación y esfuerzo por guiarme y apoyarme durante el programa de maestría y el desarrollo de este trabajo de titulación.

Hoy puedo decir que me siento feliz y agradecida con todas las personas que de una u otra forma aportaron positivamente para cumplir una de mis metas.

Marilú

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

RESUMEN

El presente trabajo tiene como objetivo establecer un modelo de preservación de documentos electrónicos a largo plazo. Se analizaron leyes, reglamentos o estatutos vigentes relacionadas con la preservación de documentos informáticos que permita la verificación de integridad de documentos informáticos para la implementación de un modelo de preservación digital de datos documentales utilizando ISO/IEC 27001. La finalidad del análisis de los modelos de preservación digital de documentos es cubrir la necesidad desde la perspectiva funcional, de organización y niveles de estado de prácticas de preservación digital para apoyar la definición de un modelo con elementos funcionales, conceptuales y de buenas prácticas que sirvan de argumentos clave para integrar una propuesta de estrategia de preservación. La investigación presenta un enfoque cuantitativo debido a que responde preguntas de investigación sobre preservación digital de documentos y sus retos actuales, que permitieron establecer dicho modelo de preservación. Para la evaluación de este análisis, se realizó la comparación de resultados antes y post implementación y se concluye que en la primera fase se obtuvo un resultado del 33,33% que las personas desconocen sobre el tema de preservación digital y luego de la implementación se obtuvo 62,67%; teniendo un nivel favorable de aceptación que corresponde que si existe un Modelo que permite realizar la preservación digital a largo plazo. Se concluye que el Modelo de Preservación Digital que se propone implementar es el modelo PREDECI, ya que cumple con todos los requerimientos funcionales de las directrices de la UNESCO, los parámetros de la Norma ISO/IEC 27001 y los criterios de NESTOR, logrando así garantizar la información de los objetos digitales.

Palabras Clave: <NORMA ISO/IEC 27001>, <INTEGRIDAD DE DOCUMENTOS INFORMÁTICOS>, <INTEGRIDAD DE DOCUMENTOS DIGITALES>, <PRESERVACIÓN DIGITAL DE DOCUMENTOS>, <MODELO PREDECI>

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
Nombre de reconocimiento (DN): c=EC, l=RIOBAMBA, serialNumber=0602766974, cn=LUIS ALBERTO CAMINOS VARGAS
Fecha: 2021.10.18 08:55:03 -05'00'

ABSTRACT

Electronic documents present several fundamental differences with traditional documents, evidencing the need for special treatment to preserve their integrity over time. Therefore, the objective of this work is to establish a model for the preservation of electronic documents in the long term. Existing laws, regulations or statutes related to the preservation of computer documents allowing the verification of the integrity of computer documents for the implementation of a model of digital preservation of documentary data using ISO/IEC 27001 were analyzed. The purpose of the analysis of digital document preservation models is to cover the need from the functional, organizational and state-of-the-art perspective of digital preservation practices to support the definition of a model with functional elements. concepts and good practices that serve as key arguments for integrating a proposed preservation strategy. The research presents a quantitative approach because it answers research questions about digital preservation of documents and their current challenges, which enabled such a preservation model to be established. For the evaluation of this analysis, the comparison of the results before and after implementation is made and it is concluded that in the first phase a result of 33.33% was obtained that people do not know about the topic of digital preservation and after the implementation was obtained 62.67%; Having a favorable level of acceptance that corresponds to if there is a Model that allows to realize digital preservation in the long term. In this case, it is concluded that the Digital Preservation Model proposed to be implemented is PREDECI model, since it meets all the functional requirements of UNESCO guidelines, the parameters of ISO/IEC 27001 standard and NESTOR criteria, thus ensuring the information of digital objects.

Keywords: <ISO/IEC 27001 STANDARD>, <COMPUTER DOCUMENT INTEGRITY>, <DIGITAL DOCUMENT INTEGRITY>, <DIGITAL DOCUMENT PRESERVATION>, <PREDECI MODEL>

CAPÍTULO I

1. INTRODUCCIÓN

En la actualidad existen Tecnologías de la Información y Comunicación (TIC) que permiten mejorar la preservación de los documentos físicos y digitales, a su vez estos continúan mejorando y creciendo en capacidad para almacenamiento de la información a bajo costo; los variados dispositivos y medios para almacenamiento ponen hoy en día al alcance de personas y organiza la capacidad de almacenar millones de bytes de información de tipo texto, imágenes, música, videos, etc.; anteriormente los archivos estaban expuestos a deterioro debido a sus materiales como papel, pergamino, fotografía, el deterioro se genera por una variedad de factores y agentes externos, la solución más factible es generar medidas preventivas para los archivos físicos y digitales basados en las características de su material, control del medio ambiente, las condiciones de almacenamiento, uso, manipulación y prepararlos antes desastres.

Estos avances tecnológicos han facilitado la producción de información, y los beneficios son múltiples, uno de ellos indica el ahorro de grandes espacios de almacenamiento que eran necesarios antiguamente cuando se conservaba la información en soporte papel, facilitado la consulta y recuperación de datos en forma casi inmediata. El soporte digital se convirtió en un facilitador para el acceso a la información, donde los gobiernos y los entes rectores de políticas de información y archivos han creado normas para acceder sin mayores contratiempos porque se estimula la calidad y efectividad del servicio al usuario o al ciudadano que requiere de datos para completar una consulta.

Es importante mencionar que el avance informático permite crear, modificar, compartir, almacenar y clasificar la información según su importancia; de manera preventiva se realiza procedimientos formales que ayuda a organizar, preservar y acceder de manera segura a la información en sus distintos formatos digitales a largo plazo. La preservación digital es una actividad dentro de las organizaciones que permite hacer una gestión de archivos donde se evitan riesgos digitales ocasionados por errores humanos, obsolescencia tecnológica, desastres naturales y problemas de tipo informático que causan la pérdida de datos e información en las estructuras de contenidos con composición binaria digital.

Cabe mencionar que el sistema de gestión documental puede ser descrito como una ventaja para la institución u organización convirtiéndose en una herramienta necesaria y de fácil acceso para los colaboradores que la utilicen, y se la puede considerar como un sistema de archivo, digitalizado y almacenado de manera automatizada; eran obtenidos de documentos electrónicos, imágenes de documentos escritos, fotografías que estaban originalmente en papel y que ya se encuentran en formato digital. El sistema de gestión documental es un conjunto de normas, técnicas y prácticas usadas para administrar el flujo de documentos en la institución u organización, que permite la recuperación de información a través de ellos, eliminar y movilizar los archivos de acuerdo a los departamentos que lo soliciten.

No todas la organizaciones o instituciones están obligadas a la conservación de su información digital, con el pasar del tiempo pueden liberar públicamente dicha información; existen obligaciones legales o institucionales que deben ser aplicadas como la protección de datos personales o normativas de derecho de autor, que provocan que la información conservada digitalmente no sea accesible por todo el público si no está limitada a un grupo específico. Para lo cual se utiliza información relacionada con antecedentes, datos, conocimientos, estrategias y alternativas sugeridas para contrarrestar la pérdida de la información, a partir de la implementación de instrucciones, herramientas y políticas se debe poner en práctica actividades que faciliten su posterior recuperación.

La conservación o preservación digital es un conjunto de actividades que son administradas para asegurar el acceso a los documentos o información digital, por un período de tiempo que sea necesario, especialmente al largo plazo y son acciones solicitadas para mantener el acceso a los materiales digitales aún después de que se presenten problemas o inconvenientes en los medios de almacenamiento o haya cambios tecnológicos. La preservación a largo plazo implica garantizar la información a través del tiempo, sin importar cuál sea su medio y forma de registro o almacenamiento aplicando diferentes parámetros a los documentos digitales con su medio correspondiente en cualquier etapa del ciclo de vida del archivo.

1.1. Planteamiento de Problema

Es evidente el mundo digitalizado en el que se está viviendo debido al impacto de las tecnologías que han revolucionado la escritura, la impresión, el habla, el sonido, la imagen, el acceso y el uso de los datos. Así la teoría del acceso, el modelo dinámico, la complejidad, la convergencia, la tecnología y representación se reflejan en los cambios de la gestión de los recursos que hoy son

representados y recuperados en un ambiente digital informacional, tipos de documentos, normas, tecnologías, objetos y software. (Álvarez-Wong, 2017)

Debido a estas circunstancias, "El patrimonio documental enfrenta severas amenazas: el saqueo y la dispersión, el comercio ilícito, la destrucción, así como la frágil particularidad de su soporte, la obsolescencia del almacenamiento y la falta de financiamiento. Según los antecedentes de creación del Programa, esta situación está provocando que gran parte del patrimonio documental haya desaparecido para siempre y otra parte importante esté en peligro." (UNESCO, 2017)

La información digital se ha convertido en una parte indispensable de nuestro patrimonio cultural y científico. Los hallazgos científicos, documentos históricos y logros culturales son cada vez más presentado en forma electrónica, y en muchos casos exclusivamente así. Sin embargo, a pesar de lo irrefutable beneficios ofrecidos por el contenido digital, hay una serie de desventajas asociadas. Los usuarios deben invertir una gran cantidad de esfuerzo técnico para acceder a dicha información. Tecnología subyacente que continúa experimentando un desarrollo a un ritmo excepcionalmente rápido y la rápida obsolescencia de tecnologías de acceso combinadas con deterioro físico a veces imperceptible de los medios de almacenamiento representan una grave amenaza para la preservación del contenido de la información, tanto contemporáneamente y en el largo plazo.

Thurston menciona los obstáculos enfocándose en los datos e información digital de los gobiernos y administraciones públicas, señala cinco obstáculos o retos en torno a la preservación digital:

- ✓ La preservación digital no es considerada como prioridad de desarrollo, por ello no es prioritario para las naciones ni cuenta con grandes fuentes de financiamiento
- ✓ Igualmente, la digitalización y los procesos de automatización, son vistos pensando sólo en el presente y no con enfoque a futuro.
- ✓ Falta de concientización por parte delos planificadores y los interesados sobre los problemas de acceso a futuro, pues creen que la tecnología resolverá todo.
- ✓ Existencia de un vacío en el marco legal e institucional, en muchos países la legislación no es clara, es inadecuada y/o desactualizada, tampoco existen políticas nacionales ni han introducido y/o aplicado normas internacionales.
- ✓ Falta de capacidad práctica para el manejo y preservación de recursos digitales, dado que existen pocos profesionales con experiencia suficiente en la gestión y preservación de estos recursos.
- ✓ Las iniciativas de digitalización son susceptibles a fallar debido a la falta de preparación adecuada y adopción de estándares. (Anne, Thurston, 2012)

A nivel mundial y principalmente en países desarrollados, organizaciones y sectores especializados en la gestión de conocimiento e información han integrado ya desde hace algunas décadas la conciencia operativa y cultura activa sobre la importancia de establecer protocolos, actividades y colaboraciones formales orientadas a la preservación de sus memorias y patrimonio digital. Institutos, gobiernos y organizaciones mundiales como la NASA, UNESCO, Massachusetts Institute of Technology (MIT), Harvard, Library of Congress, IBM, Stanford University, National Library of Australia o Koninklijke Bibliotheek, han desarrollado investigación, sistemas y modelos de trabajo orientados a mantener el acceso permanente y a largo plazo del patrimonio documental de contenidos nacidos digitalmente y materiales digitalizados. (Leija Román, 2017)

Ecuador como muchos países no posee políticas, normativas, estrategias específicas que regulen la preservación a largo plazo de la documentación digital, existen leyes como la Ley del Sistema Nacional de Archivo, la Norma de Gestión Documental para Entidades de Administración Pública y estatutos propios de las empresas e instituciones que no posee una normativa específica o un modelo que garantice la Preservación a Largo Plazo de Documentos Digitales, pero el artículo 4 de la Ley del Sistema de Registro de Datos Públicos, señala: "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información". (Públicos, 2012)

Para el caso de Instituciones Educativas de Educación Superior las cuales se rigen por el Consejo de Educación Superior en su Título III Tratamiento de la Documentación Capítulo I De La Transferencia de a Documentación, en su Artículo 23 De la Preservación y Salvaguarda de los Documentos estipula en una parte que “La documentación de carácter histórica se digitalizará como medida de preservación, poniendo a disposición en el software especializado la información para estudios e investigación a fin de minimizar la manipulación de los documentos originales, los cuáles serán prestados para consulta solo en casos necesarios para el estudio del documento o para verificar la autenticidad del material, así como los sujetos a estudios paleográficos. De igual forma que lo indicado anteriormente, sobre el tema en las Leyes mencionadas el contenido está muy general y abierto a definiciones, sin mecanismos, ni metodologías específicas de cómo tratar la preservación de documentos y datos digitales.

Por esta razón implementar un modelo de preservación a largo plazo de datos digitales que permita mantener, proteger y resguardar de forma anticipada y permanente con gestiones específicas con el fin de asegurar la continuación y acceso del contenido de documentos digitales a largo tiempo y las tecnologías independientes de su soporte, formato o sistema y que en caso de deterioro o daño por diferentes causas se pueda restaurarlos. Por lo que este trabajo se concentra en el análisis de modelos de preservación digital para garantizar la autenticidad y trazabilidad a largo plazo de los documentos digitales.

1.2. Formulación del Problema

¿Es posible mejorar la preservación a largo plazo de documentos digitales mediante la implementación de un modelo de preservación de documentos digitales previo al análisis de modelos de Seguridad Digital de Datos?

1.3. Sistematización del Problema

¿En qué consiste y que objetivos persigue la preservación digital en el ámbito de documentos digitales como método emergente a la perdida de patrimonios culturales e intelectuales a nivel mundial?

¿Cuáles son las acciones, modelos, estrategias o políticas vigentes para la gestión de archivos de documentos digitales, preservación a largo plazo en Ecuador?

¿Qué tipos de modelos cumple con los requisitos y recomendaciones de buenas prácticas en preservación digital a largo plazo y son aplicadas internacionalmente y cuáles son las principales semejanzas, diferencias, beneficios y desventajas?

¿Cuál es el nivel de preservación digital que existe en la gestión documental de repositorios públicos de acuerdo a las políticas internacionales?

¿La implementación de un modelo de preservación digital mejorará las necesidades de almacenamiento seguro y perecedero con el fin de mejorar la accesibilidad y trazabilidad a largo plazo de los documentos digitales?

1.4. Justificación de la Investigación

1.4.1. Teórico

"El objetivo de la seguridad de la información es proteger la información de una empresa como el bien más preciado" (Shameli-Sendi, 2016). La mayoría de las veces la información de una organización es medida imaginariamente, sin tener conciencia del impacto para la empresa en el caso de pérdida, destrucción o de ser vulnerada.

Frankfurt am Main dice, la mayor parte de los documentos creados hoy en día "nacen" con formato digital, o son convertidos a formato digital mediante alguna transformación tecnológica. Los documentos electrónicos presentan varias diferencias fundamentales con los documentos tradicionales, de ahí que necesiten un tratamiento especial para preservar su integridad como documentos a lo largo del tiempo. Estas características singulares de los documentos electrónicos exigen acciones singulares de preservación. Las organizaciones deben ser conscientes de que las acciones de preservación de documentos electrónicos se inician preferiblemente en el momento de la creación de los documentos. En otras palabras, cuanto antes comience el proceso que da lugar a las actividades de preservación, mayor será la seguridad de que los documentos conservarán los requisitos de fiabilidad, integridad, autenticidad y utilidad. (NESTOR, 2009)

Para la humanidad la pérdida de la información digital tendría consecuencias desastrosas, no solo por lo que significa para el quehacer diario de la vida en sociedad, sino también por las consecuencias que provocaría en la continuidad del conocimiento, a la memoria y a la identidad del ser humano, los grupos sociales, los países y las áreas geográficas en que convivimos. (Álvarez-Wong, 2017)

Para Aquino uno de los mayores problemas es que se piensa más en el corto plazo que en el largo plazo, al mismo tiempo, el consumismo imperante en el mercado ha aumentado la obsolescencia de programas y equipos tecnológicos que son necesarios para la visualización de los documentos digitales. En este sentido, uno de los retos más álgidos para el futuro de la preservación de recursos digitales será el contar y tener operativos la cantidad necesaria de software y hardware que hagan posible la lectura de archivos digitales. Cabe resaltar que además de los factores tecnológicos en la preservación digital están implicados una serie de factores legales y documentales. (Aquino, 2016)

Juan Voutssas menciona que "la preservación de documentos de archivo se define como: el conjunto de principios, políticas, reglas y estrategias que rigen la estabilización física y tecnológica, así como la protección del contenido intelectual de documentos de archivo

adquiridos, con objeto de lograr en ellos una secuencia de existencia a largo plazo continua, perdurable, estable, duradera, ininterrumpida, inquebrantada, sin un final previsto. Para documentos de archivo digitales se agrega a la definición en el caso de preservación documental digital debe establecerse específicamente cómo esos documentos serán conservados durante y a través de las diferentes generaciones de la tecnología a través del tiempo, con independencia de donde residan, su soporte y de sus formatos. (Voutssas, 2010)

La UNESCO menciona: en la Carta para la preservación del patrimonio digital en el artículo 3 de la misma se reconoce el peligro de pérdida a que están sometidos estos materiales y se afirma: «El patrimonio digital del mundo corre el peligro de perderse para la posteridad. Contribuyen a ello, entre otros factores, la rápida obsolescencia de los equipos y programas informáticos que le dan vida, las incertidumbres existentes en torno a los recursos, la responsabilidad y los métodos para su mantenimiento y conservación y la falta de legislación que ampare estos procesos». (UNESCO, Directrices para la Preservacion del Patrimonio Digita, 2003)

La adopción de un modelo de red de preservación digital es una alternativa para las organizaciones que quieren coleccionar, almacenar, preservar y ofrecer acceso a su acervo en copias digitales autorizadas. También es imprescindible la concordancia de esas redes con las normas internacionales ya probadas y que promueven el archivamiento digital de la producción científica a largo plazo. (Arellano, 2013) Molina y Rodríguez dicen: "Cada modelo de preservación digital funciona de manera diferente; estos modelos se aplican a entornos específicos. Algunos modelos se limitan a ciertos tipos de objetos digitales, algunos se centran en soluciones específicas, mientras que otros describen las interacciones funcionales a un alto nivel y tienden a describir soluciones absolutas". (Molina Fernando y Rodriguez Glen , 2017) Señala M. Termens que: "en lugar de optar por el diseño de un *software* determinado se optó por la creación de un modelo teórico de carácter general que asegurara la preservación y el acceso a la información" (Termens, 2013).

Por esta razón, en el documento elaborado para la UNESCO por la Biblioteca Nacional de Australia, que contiene directrices generales y técnicas para la preservación del creciente patrimonio digital mundial y el acceso permanente al mismo. Tiene por finalidad servir de manual de referencia sobre el Proyecto de Carta para la Preservación del Patrimonio digital, que se han convertido en el inicio y unificación para que muchos países de estrategias y guía para proyectos de preservación de documentos a largo plazo.

La implementación de un Modelo de Preservación Digital a Largo Plazo que mejore el aseguramiento del acervo intelectual que manejan y constituya en una pauta para el qué, cómo y

durante cuánto tiempo se resguardaran los documentos digitales, y que permita llegar a cumplir los principios de la preservación digital como la integridad, autenticidad, fiabilidad, funcionalidad de la información, evitando perdida o destrucción de patrimonio intelectual.

1.4.2. Metodológico

El desarrollo de este proyecto se combina por una investigación de tipo exploratoria y descriptiva integrada por procedimientos mixtos de enfoque cualitativo, de manera diferenciada y progresiva en sus distintas fases se integran técnicas de investigación como la revisión bibliográfica, la observación comparativa, el cuestionario, el test y la entrevista.

La metodología con la que se realizará el análisis de los modelos, es estudiar las estrategias, políticas, normas, técnicas, estándares, leyes, estatutos existentes de preservación de documento digitales internacionales y locales con el objetivo de implementar un modelo que cumplan con las características de una preservación duradera en el tiempo y que se adopten las mejores prácticas en personas e instituciones desde el inicio de la creación de los documentos digitales para evitar gastos futuros y perdidas de información.

Para alcanzar los objetivos planteados es necesario realizar una revisión bibliográfica literaria de la Preservación Digital, luego se realizará un estudio del estado de las instituciones tecnológicas en cuanto a la preservación digital, también se analizará los modelos de preservación digital a largo plazo para realizar la selección de las mejores normativas, estándares, políticas y así definir e implementar la mejor propuesta para el proceso de preservación.

1.4.3. Práctico

Con la implementación de un Modelo de preservación digital de datos documentales se proveerá los lineamientos para mejorar la preservación de los datos intelectuales producidos por los estudiantes de los ITES. El tema de investigación propuesto se alinea con la Norma de Gestión Documental para Entidades de Administración Pública; con la resolución N20 NG-DINARDAP-2013 de la Dirección Nacional de Registros Públicos; con El Programa Memoria del Mundo de la UNESCO este indicará específicamente los parámetros a seguir a la persona que se encuentre a cargo de del resguardo del archivo documentos digitales.

1.5. Objetivo

1.5.1. Objetivo General

Analizar la seguridad informática e información basado en la norma internacional ISO/IEC 27001 para diseñar un modelo que permita la verificación de integridad de documentos informáticos.

1.5.2. Objetivos Específicos

- Analizar las leyes, reglamentos o estatutos vigentes relacionadas con preservación de documentos informáticos.
- Estudiar los modelos de preservación digital documental para asegurar los datos a largo plazo como PREDECI, OAIS, PREMIS, DAMM
- Proponer un modelo utilizando ISO/IEC 27001 que permita la verificación de integridad de documentos informáticos
- Evaluar del modelo propuesto de preservación digital.

1.6. Hipótesis

¿La implementación de un modelo basado en la norma internacional ISO/IEC 27001 permitirá obtener la integridad de documentos informáticos?

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos

Como referencia para el desarrollo del proyecto se recurre a los estudios y artículos científicos realizados sobre temas afines a la preservación de documentos más relevantes que respaldan la investigación y constituyan métodos de análisis. Entre estos trabajos se tienen los siguientes:

En el artículo científico realizado por (Molina Fernando y Rodriguez Glen , 2017) con el tema "The preservation of digital evidence and its admissibility in the court", analiza los modelos comunes de preservación digital que existen, los elementos, el grado de cumplimiento de las pautas generales, el uso de técnicas y el cumplimiento de requisitos específicos, así como evaluar la necesidad de una solución al problema.

La conclusión que aportó este estudio fueron:

> Las cuestiones ignoradas por los modelos actuales de preservación incluyen el museo de herramientas, terminología, control de calidad de la ingesta, evidencia de entorno de metadatos de ingesta parcial para preservar y garantizar la integridad del original, evaluación de riesgos, almacenamiento distribuido, preservación del tiempo, certificaciones de la estrategia, legalidad de la evidencia, respecto por los derechos fundamentales, la confiabilidad y efectividad de la evidencia, respecto por las reglas de protección de datos y secreto de las comunicaciones, respecto por el derecho a la libertad de expresión, confidencialidad, preservación de roles, gestión de roles, control de evidencia física, transmisión, trazabilidad, y continuidad de preservación. Es necesario demostrar que ningún modelo cumple con todos los parámetros, requisitos, principios y estándares mínimos establecidos para preservar la evidencia digital en las instituciones de investigación criminal.

Por otro lado, el artículo científico realizado por (Álvarez-Wong, 2017) con el tema "The digital repositorios for conservation. An approach to the digital long-term preservation", pretende contribuir a la formación de criterios relacionados con la preservación digital a largo plazo, al conocimiento de los repositorios digitales, así como sugerir un conjunto de medidas generales que permita trazar una acertada estrategia para la preservación de la información digital.

Aportando con las siguientes conclusiones:

> Un punto crítico para información digital se encuentra la obsolescencia tecnológica, la fragilidad tecnológica, la rápida actualización de las tecnologías, la caducidad de software y formatos, la dependencia tecnológica y la pérdida de funcionalidades.
>
> No hay una solución práctica aplicable universalmente al problema de la obsolescencia tecnológica de los materiales digitales y es poco probable que se encuentre una solución única que ofrezca un medio de acceso económico a todos los materiales, para todos los fines y en todo momento.
>
> El uso intensivo de la nube para almacenar los documentos digitales en Internet aumenta el problema de la preservación digital porque hay que garantizar que se controlen los metadatos de integridad, la cadena de custodia, retención y disposición, transferencia y recuperación, control intelectual, así como la autenticidad, la fiabilidad y confiabilidad de los documentos en línea.
>
> La concientización de la necesidad de establecer políticas de preservación en el medio digital que definan su alcance en correspondencia con los objetivos de las instituciones, establezcan los responsables de aplicarlas para que sean utilizadas como instrumento de gestión en la salvaguarda y garanticen la política de la organización, las responsabilidades asignadas, los calendarios de conservación y de eliminación, y los manuales de procedimientos.

En la tesis de investigación realizada por (Giusti, 2014) con el tema "Una metodología de evaluación de repositorios digitales para asegurar la preservación en el tiempo y el acceso a los contenido" de la Universidad Nacional de la Plata: propone "una metodología de evaluación para repositorios institucionales se relevaron los modelos que a lo largo del tiempo han servido para representar un repositorio digital". Donde busca mejorar la calidad de los repositorios, así como la estandarización, ayudar a la interoperabilidad y obtener una mayor visibilidad de las producciones que una institución educativa guarda en un repositorio, así como asegurar la preservación de los contenidos del repositorio, de modo que siempre sea posible acceder a ellos y que éstos resulten legibles tanto para usuarios humanos como máquina.

De igual manera, este trabajo investigativo aporta con las siguientes conclusiones más relevantes:

> Se determinó el cumplimiento del repositorio en relación a los elementos constitutivos del paquete de información del modelo OAIS de la norma ISO 14721, que es el modelo

a seguir para demostrar las capacidades del repositorio y sus falencias. Cada una de las partes del modelo abstracto del paquete de información (información de contenido y su representación; información descriptiva de la preservación; información descriptiva) fue contrastada siguiendo el método propuesto en este trabajo.

Se realizó el perfilamiento de todos los objetos del repositorio, determinando su riesgo de preservación en función de los formatos existentes y estipulando asimismo acciones que ya han sido iniciadas para mejorar el estado de los ítems (acciones de conversión, migraciones, presentación de estándares y elección de formatos para exposición y preservación de los ítems).

En relación a la información descriptiva de la preservación, además de trasladar el modelo abstracto de la PDI a la realidad de los metadatos en el repositorio, que dan cuenta de los cinco elementos (integridad, fijeza, procedencia, contexto y derechos), se desarrolló un validador y se establecieron las reglas con las que cotejar el cumplimiento con la PDI.

En el informe realizado por (Webb, 2003) con el tema "Directrices para la Preservación del Patrimonio Digital" de la Biblioteca Nacional de Australia para la UNESCO: que contiene directrices generales y técnicas para la preservación del creciente patrimonio digital mundial y el acceso permanente al mismo y tiene por finalidad servir de manual de referencia sobre el Proyecto de Carta para la Preservación del Patrimonio digital.

El aporte del siguiente proyecto es:

Estrategias para preservar los objetos digitales.

- Colaborar con los productores (creadores y distribuidores) para aplicar normas que prolonguen la vida efectiva de los medios de acceso y reduzcan la variedad de problemas desconocidos que deben ser tratados.
- Reconocer que no es realista tratar de preservar todo y que hay que seleccionar el material que debe ser preservado.
- Guardar el material en un lugar seguro.
- Controlar el material utilizando metadatos estructurados y otros documentos que faciliten el acceso y ayuden durante todo el proceso de preservación.
- Proteger la integridad y la identidad de los datos.
- Elegir los medios apropiados para proporcionar acceso pese a los cambios tecnológicos.

- Administrar los programas de preservación para que alcancen sus objetivos de manera económica, oportuna, global, dinámica y responsable.

En el artículo realizado por (Giménez, 2014) con el tema "Criterios ISO para la Preservación Digital de los Documentos de Archivo" de la Universidad Politécnica de Valencia, España: donde tiene como objetivo identificar qué diferencias o semejanzas existen entre la actividad de preservación o conservación de los documentos físicos y digitales, para, por un lado, contextualizar las acciones y los elementos de la preservación digital y, por otro, analizar las principales propuestas que realizan diferentes normas ISO para que las organizaciones implementen un programa de preservación digital que garantice la usabilidad de los documentos a lo largo del tiempo.

Entre las conclusiones con las que aporta este artículo se tiene:

> Las normas ISO proponen soluciones y acciones que se deben realizar para garantizar que los documentos digitales se conserven a lo largo del tiempo, en tanto las organizaciones consideren que son esenciales como evidencia de su patrimonio o actividades y deseen garantizar su autenticidad, integridad y usabilidad en todo ese tiempo.
>
> Cualquier organización productora de documentos digitales debe diseñar una estrategia para asegurar su conservación y disponibilidad, en función de afrontar los riesgos de la obsolescencia tecnológica. Es imprescindible que dichos documentos estén organizados, clasificados, descritos e indizados, para poder ser identificados y recuperados de la forma más pertinente en el momento en que se desee. Para asegurar la protección de los documentos electrónicos y su autenticidad, se recomienda que estos no sean dependientes del software que los creó y, además, que sean convertidos al formato .pdf/a, con la incorporación de metadatos. Mediante los metadatos insertados en los documentos digitales se asegura su identificación, por lo cual se debe incorporar información relacionada con la fecha y hora de creación, su creador, el calendario de conservación, su clasificación y relación con otros documentos, etc. Estos metadatos también se pueden almacenar en un repositorio y deberían poder extraerse de los formatos propietarios mediante el lenguaje de marcas .xml.
>
> En cuanto al almacenamiento de los documentos digitales, se debe asegurar un soporte estable contra la obsolescencia tecnológica que, a su vez, permita las migraciones a nuevos soportes, con la completa garantía de que se protege la información, sin pérdidas ni alteraciones del contenido. El proceso de migración debe realizarse con una metodología acorde con unos controles de calidad.

Si se desean enviar documentos electrónicos de un sistema de almacenamiento a otro o en un sistema de gestión documental, la información debe ser encapsulada mediante un paquete de información de archivo, como indica la norma OAIS, cuyos principales componentes son el contenido del documento y sus metadatos, lo que permitirá su preservación a largo plazo.

2.2. Preservación Digital

La preservación digital son técnicas o procesos que provienen del campo de la informática que son necesarios para conservar en el tiempo objetos digitales en un sistema de información, también se ocupa del almacenamiento de datos, así como de su integridad para que se pueda recuperar en el tiempo una copia exacta de la información previamente introducida.(Juan José Boté, 2012, p. 38)

La preservación digital se basa en la "aplicación de técnicas activas de conservación informática por que ante la aparición de un problema es posible que no se tenga una solución, o ante un borrado de datos no se tenga una restauración".(Yolanda Alvear & Liliana Abelló, 2019, p. 36)

La digital preservation coalition (DPC) se refiere a la preservación digital como el manejo de todas las actividades necesarias para asegurar el acceso continuo a materiales digitales por el tiempo que sea necesario. Son todas las acciones requeridas para mantener el acceso a materiales digitales más allá de los límites de las fallas de medios o cambios tecnológicos; los tiempos de resguardo y acceso a material digital son la parte fundamental en la línea de vida de la preservación digital.(Davis Leíja Román, 2017, p. 32)

2.2.1. Principios de la Preservación Digital

Tabla 1-2 Factores que no permiten la Preservación Digital a Largo Plazo de archivos Digitales

Principio	***Concepto***
Integridad	Asegura que el contenido informativo, la estructura lógica y el contexto no se han modificado ni se ha afectado el grado de fiabilidad ni la autenticidad del documento original. "La integridad de un documento de archivo debe estar completo e inalterado en todos sus aspectos esenciales. Junto con la identidad, conforma la autenticidad del documento".

Equivalencia	Los documentos electrónicos manifiestan la obsolescencia, cualquier modificación se puede considerar valida siempre que garantice que mantiene intacto el contenido de la información, la estructura lógica y su contexto que le garantice ser documento original.
Economía	Se debe aplicar procesos, procedimientos, métodos y técnicas de preservación digital de manera viable, sostenible, práctico y apropiados para el contexto de documentos, de tal forma que se asegura la sostenibilidad técnica y económica de la preservación digital.
Actualidad	Esto debe evolucionar al ritmo de la tecnología y utilizar los medios disponibles en el momento que garantiza la preservación de los documentos en un futuro. Esto quiere decir que el sistema de preservación digital debe mantener la capacidad de evolucionar, ajustarse a los cambios en las dimensiones y añadir nuevas presentaciones y servicios.
Cooperación	Reutiliza y comparte soluciones ya existentes y desarrolladas de manera conjunta con otros archivos digitales, especialmente con los procesos que pueden ser gestionados de manera centralizada.
Normalización	Se genera lineamientos y herramientas basadas en normas, estándares y buenas prácticas.

Fuente: Yolanda Alvear & Liliana Abelló, 2019, p. 37 y Claudia Castillo, s. f., p. 17

Tabla 2-2: Factores de la Preservación Digital

Factor	*Concepto*
1. Factor Cultural	Tiene que ver con el aspecto social y la falta de sensibilidad, así como el desconocimiento, ausencia, pérdida de información esto se debe por la falta de medidas para la preservación digital a largo plazo, no se pensaba en el futuro y evidencias para futuras generaciones.
2. Factor Social	Son las actividades y ejercicios que garantizan el acceso y uso de los documentos, quiere decir que usuarios y comunidad en general puede acceder a la información sin restricciones.
3. Factor Tecnológico	Son todos los componentes que ayudan al contexto de las tecnologías de la información en los cambios permanentes ocasionando preocupación en la duración de soportes y el origen de las obsolescencias tecnológicas como amenaza a la información.
4. Factor Documental	La metodología archivista se ha modificado con la información digital, se debe establecer entre los profesionales otras dinámicas para la creación, conservación, preservación y recuperación documental. La preservación garantiza la permanencia en el tiempo, así como los metadatos forman parte de la calidad del documento que se va a preservar y su debido manejo en la recuperación y permanencia del mismo.
5. Factor Legal	Son aspectos jurídicos relacionados con los creadores, autores de la información en el contexto digita. A nivel mundial se ha desarrollado normas o políticas para evitar la piratería de editores,

	dado que la información para los usuarios esta dado con mayor facilidad por esta razón se establece controles para la protección del derecho de autor.
6. Factor Económico	Es el factor económico de los proyectos, para asegurar la información a largo plazo, permite establecer modelos económicos que tengan viabilidad para establecer políticas de preservación.

Fuente: Yolanda Alvear Guerrero & Liliana Abelló Hernández, 2019, p. 38,39

Existen cinco factores sobre los que se debe prestar especial atención porque puede que no permiten la preservación a largo plazo de los archivos digitales. Estos factores son: factor cultural, factor tecnológico, factor legal, factor social y factor económico:

Tabla 3-2: Factores que no permite la preservación a largo plazo de archivos digitales.

	Factor Cultural	***Factor Tecnológico***	***Factor Legal***	***Factor Social***	***Factor Económico***
Lo que observa	La sociedad no valoran su patrimonio	El rápido desarrollo tecnológico	Buscar un equilibrio entre el derecho a la información y el derecho de autor.	Garantías de acceso y usabilidad de la información.	Definir los costos según los criterios
Lo que genera	La necesidad de no salvaguardar el patrimonio	La problemática de la conservación de los bits, y el cómo hacerlos legibles a largo plazo.	Buscar un dialogo entre las necesidades de distribución, reguardo y protección de la información y sus características legales.	Buscar mecanismo para que se pueda acceder de manera efectiva y masiva a la información.	Sistematizar los criterios de valoración de la información que se busca preservar con el costo de su preservación.
Consecuencias	Pérdida de acervo documental	Pérdida de información. Los formatos y equipos se hacen obsoletos con el pasar del tiempo. Seguridad de la Información (preservación, error de registro, sustracción, manipulación de la información).	Determinar si existe o no flexibilidad en los derechos de autor y su alcance.	Determinar el tipo de público para cada acervo de información.	Asegurar que la información no se pierda a largo plazo por el criterio económico.

Fuente: Jennifer Sánchez Salazar, 2019, p. 20

El término preservación digital debe ser unificado y a su vez diferenciado de los conceptos de conservación y seguridad informática. La conservación pone énfasis en establecer unas condiciones ambientales, de almacenamiento y uso que permitan conservar un documento en las mejores condiciones posibles de estado físico. Las técnicas de conservación que son empleadas principalmente en documentos analógicos son también de aplicación en los documentos digitales. La seguridad informática se encarga de establecer políticas para análisis, detección y prevención de posibles riesgos de tipo informático que puedan sufrir los datos de origen informático estableciendo procedimientos de copias de seguridad, control y autorización de acceso, así como de análisis y detecciones generales de fiabilidad en el software y hardware utilizado.(David Leíja Román, 2017, p. 33)

Tabla 4-2: Dimensiones y necesidades en preservación digital

Dimensiones y Necesidades PD	***Datos***	***Tecnología***	***Economía***	***Legales***	***Normativas***	***Organización***
Institucional	Grandes cantidades y tipos de datos e información.	Altas necesidades de tecnología informática.	Alto nivel de inversión y mantenimiento a largo plazo.	Información propiedad de la institución y de externos.	Alta necesidad de normalización de información.	Grandes grupos y personal.
Empresarial	Medianas y grandes cantidades y tipos de datos e información.	Altas necesidades de tecnologías informáticas.	Alto nivel de inversión y de mantenimiento a largo plazo.	Información propiedad de la empresa y de externos.	Alta necesidad de normalización de información.	Medianos grupos y personal.
Particular	Medianas y bajas cantidades de datos e información.	Bajas necesidades de tecnologías informáticas.	Mediano nivel de inversión y de mantenimiento a largo plazo.	Información propiedad particular.	Baja necesidad de normalización de información.	Pequeños grupos particulares.

Fuente: David Leíja Román, 2017, p. 32

2.2.2. Tipos de Preservación Digital

La preservación digital es una serie de actividades bien aseguradas para el acceso continuo a los materiales digitales a pesar de cualquier situación o riegos que se pueden presentar y esta se clasifica en tres grupos de acuerdo al tiempo:

Tabla 5-2: Plazos en preservación digital a nivel conceptual DPC

TIEMPO	*DEFINICIÓN*
Preservación a corto plazo (short-term preservation)	Acceso a los materiales digitales en un periodo de tiempo definido o que sea menor a los cambios tecnológicos.
Preservación a mediano Plazo (médium-term preservation)	Acceso continuo a los materiales digitales aun después de los cambios tecnológicos en un periodo definido de tiempo, pero no indefinidamente.
Preservación a largo plazo (long-term preservation)	Acceso continuo e indefinido al material digital o al menos a la información que contiene.

Realizado por: Marilú Torres, 2021
Fuente: Yolanda Alvear Guerrero & Liliana Abelló Hernández, 2019, p. 38

2.2.3. Estrategias de Preservación Digital

2.2.3.1. Conservación

Son los documentos digitales que se encarga de la preservación del contenido como de la apariencia, en la actualidad se han generado nuevas versiones de bases de datos, hojas de cálculo y procesadores de texto que poseen correcciones y actualizaciones; se puede decir que preservar la apariencia de un documento digital es difícil cuando se trata de texto, pero es casi imposible cuando se trata de entornos multimedia, donde hay una intensa interrelación entre hardware/software y contenidos. (Plan de Preservación Digital, 2020)

2.2.3.2. Digitalización

Es la técnica por la cual un objeto análogo, independiente de su forma, se transforma en digital, y es legible mediante un sistema de computación, existen algunos procesos que se le puede considerar dentro de este campo el fotografiado digital, escaneo de documentos y el uso de reconocimientos ópticos de carácter. Se debe tener en cuenta el formato digital de salida y cual se adecua a las necesidades de la unidad de información, institución u organización. Debe quedar en claro que no solo el papel se digitaliza sino también las fotografías en papel, diapositivas, posters, cintas de video, cintas de audio, películas de cine de 8mm o de 35mm, entre otros. (Juan José Boté Vericad, 2012, p. 46)

2.2.3.3. Documento de Archivo

Son los registros de información generada o recibida por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, científico, histórico, técnico o cultural y debe ser objeto de conservación en el tiempo, con fines de consulta posterior. (*Plan de Preservación Digital*, 2020, p. 10)

2.2.3.4. Documento Digital

Es la información representada por medio de valores numéricos diferenciados - discretos o discontinuos, por lo general valores numéricos binarios (bits), de acuerdo con un código o convención preestablecidos. (Plan de Preservación Digital, 2020, p. 10)

2.2.3.5. Documento Electrónico

Es la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares. El documento electrónico es aquel cuyo soporte material es algún tipo de dispositivo digital que, para ser consultado, interpretado o reproducido, debe ser accedido desde un computador u otro dispositivo con capacidad de acceder a información en medios magnéticos. (Plan de Preservación Digital, 2020, p. 10)

2.2.3.6. Documento Electrónico de Archivo

Registro de información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida, por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, o valor científico, histórico, técnico o cultural y que debe ser tratada conforme a los principios y procesos archivísticos. (Plan de Preservación Digital, 2020, p. 10)

2.2.3.7. Migración

La migración es una técnica que consiste en transformar un objeto digital en otro objeto digital de une versión tecnológica superior, de manera que la información contenida pueda ser accesible mediante soporte informático diferente, teniendo como resulta una versión moderna y avanzada. Este proceso puede ocasionar pérdidas o cambios en las características de los documentos, en su apariencia a esto se lo conoce como modificación de las propiedades significativas del documento. (Juan José Boté Vericad, 2012, p. 50)

2.2.3.8. Reportes de Soporte

El refresco o actualización de soportes es una técnica que enriquece y se comparte en cierta medida con las actividades de migración digital, que implica un trabajo más complejo. La actualización debe considerar conceptos como la compatibilidad, soporte industrial, estándares de uso, factores externos, obsolescencia tecnológica, también sugiere su renovación y copia de datos digitales a un nuevo soporte, dando a entender que esta copia sugiere un sentido de identidad única la cual no estará libre de la obsolescencia ya que el formato sería el mismo y por tanto requiere de otras técnicas complementarias. (David Leíja Román, 2017, p. 68)

2.2.3.9. Emulación

Técnica que recrea la apariencia y la funcionalidad original de un objeto digital mediante la utilización de aplicaciones que simulan (emuladores) el funcionamiento de los programas (software) originales con los que fueron creados en la actualidad se encuentran obsoletos. Está siendo considerada como una alternativa a la migración. (*Plan de Preservación Digital*, 2020, p. 10)

2.2.3.10. Análisis Forense

Dispone de objetos de origen digital y permite recibir en la unidad de información soportes digitales cuyo acceso es difícil o requieren que no tengan manipulación alguna, también identifica

como se empleó por última vez el objeto digital. Esta técnica permite saber sobre qué sistema se ha creado un objeto y busca los recursos adecuados para su debido tratamiento. (Juan José Boté Vericad, 2012, p. 52)

2.2.4. Pilares de la Preservación Digital

Principios: Es el marco teórico y mejores prácticas para el desarrollo del Plan de Preservación Digital.

Política: Están constituidas por la decisión administrativa del organismo e institución, a fin de formalizar y aplicar los principios rectores en la definición del Plan de Preservación Digital.

Las políticas de preservación digital forman parte de la gestión documental. Se trata de un documento estratégico que contiene una declaración escrita y autorizada por la dirección de la organización e institución.

Estrategias: Es el conjunto de alternativas técnicas, tecnologías, prácticas y conceptuales, que están definidas como solución a las demandas generadas por el Plan de Preservación Digital a Largo Plazo. (*Plan de Preservación Digital*, 2020, p. 22)

2.2.5. Modelos de Preservación Digital

Los modelos de preservación digital son meta modelos de archivos que sugieren técnicas, estrategias y acciones de manera puntuales para ser preservados a largo plazo, existen modelos técnicos que son de referencia obligada a nivel de recomendaciones y estándares internacionales para integrar un modelo preservación digital. (David Leíja Román, 2017, p. 38)

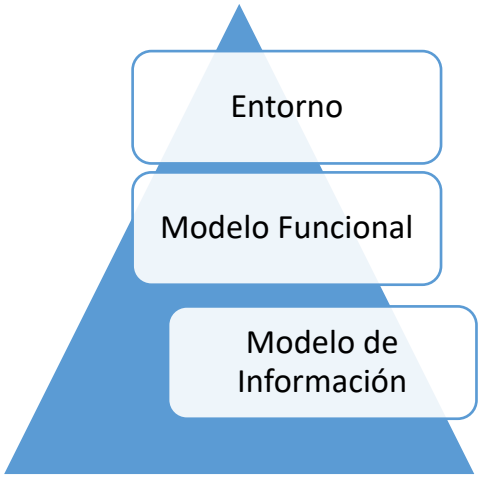
2.2.5.1. Modelo de Referencia OAIS

OAIS (Open Archival Information System) fue desarrollado en el año 2002 por Consultative Committee for Space Data Systems (CCSDS) para poderse usar en una amplia gama de organizaciones con necesidades de gestionar un archivo digital y de aquellas que principalmente tienen como objetivo organizar a personas y sistemas en un mismo entorno de trabajo para el manejo de un sistema de información de archivo con el fin de preservar a largo plazo toda la información y esta esté accesible a una comunidad designada de usuarios. Este modelo se basa en la Norma ISO 14721:2003 que integra un marco de trabajo como conceptos, recomendaciones,

normas, requerimientos la integración de acciones humanas y elementos informáticos. (David Leíja Román, 2017, p. 40)

El modelo OAIS ha sido ampliamente adoptado por las comunidades, instituciones y organizaciones interesadas en la preservación digital, en la actualidad se encuentra como referencia obligada para iniciar un esquema de orden y visualización de un plan de preservación digital, el que más utiliza este modelo son los repositorios digitales. (David Leíja Román, 2017, p. 41)

Sobre esta base el modelo OAIS establece un marco conceptual que estructura las etapas y funciones de un archivo digital a partir de 3 componentes: entorno, modelo funcional y modelo de información.



Componentes de un Archivo OAIS
Fuente: Claudia Castillo, s. f, p. 20

Entorno

Está conformado por todos los actores que están en los exteriores (afuera) del modelo OAIS como son: Productor, Directo y los Usuarios como se detalla en el siguiente gráfico.

Entorno de un archivo OAIS
Fuente: Claudia Castillo, s. f, p. 20

2.2.5.1.1. Modelo Funcional

El modelo OAIS está formado por 6 entidades funcionales:

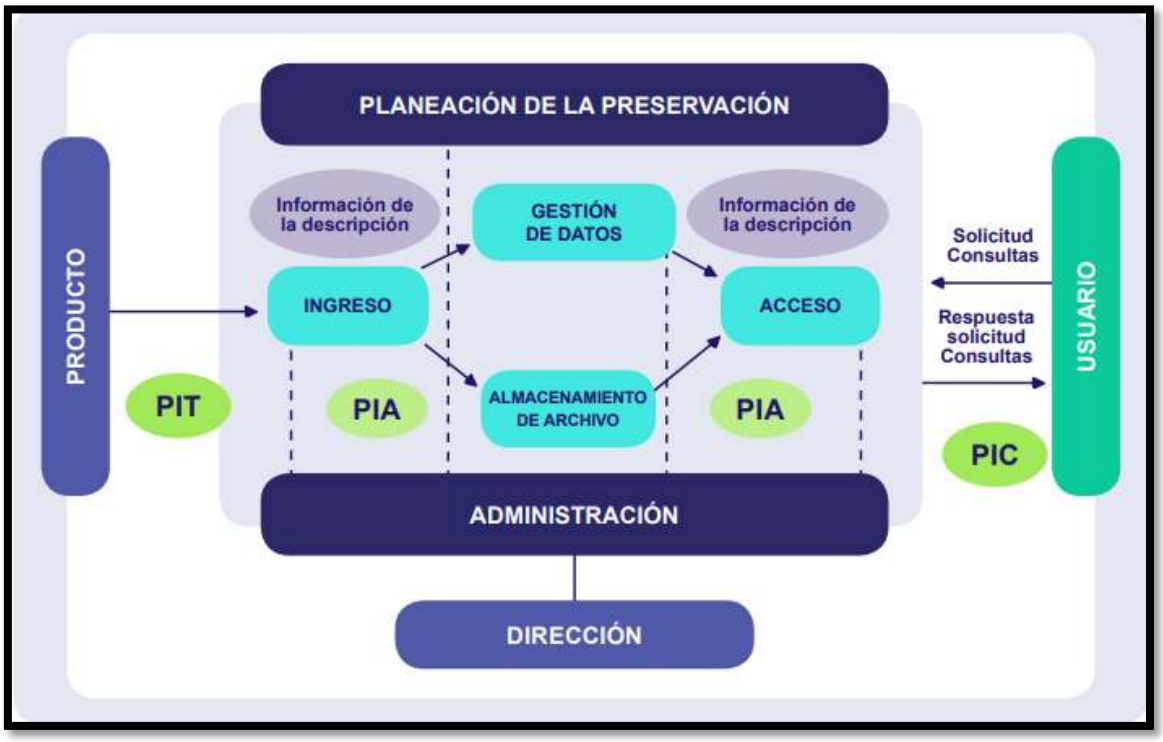


Figura 1-2: Entidades Funcionales del OAIS
Fuente: Claudia Castillo, s. f, p. 20

Entidades Funcionales del Modelo OAIS

Se describe de manera detallada todos los conceptos funcionales que integran el nivel de entidades, información objetos, etc. Describiremos los conceptos en los cuatro grupos que integran el modelo funcional como: entorno, información, entidades e interacciones.

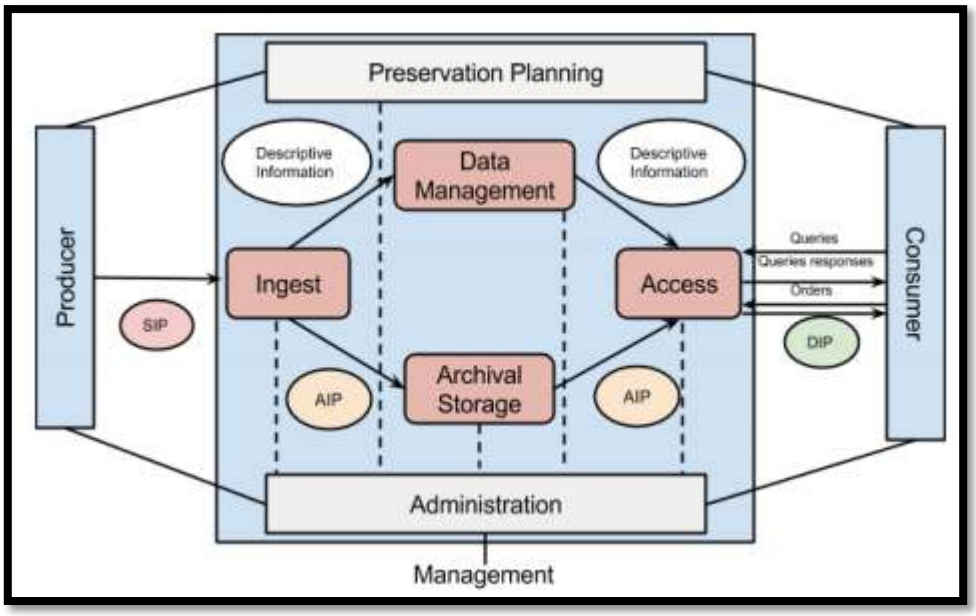


Figura 2-2: Entidades Funcionales del Modelo OAIS
Fuente: David Leíja Román, 2017, p. 43

Tabla 6-2: Entidades Funcionales del Modelo OAIS

Entidades Funcionales del Modelo OAIS				
Entorno del Modelo OAIS	Se considera parte del entorno los elementos productores, consumidor y gestión que existen fuera de OAIS como puntos activos para hacer funcionar el ciclo de funcionamiento.	**Productor (Producer)**	El productor lo ejerce las personas o el sistema cliente que provee información al OAIS, es decir que hace llegar la ingesta de información para que sea administrada y luego preservada.	
		Gestión (Management)	El manejo y gestión es un rol que integra todas las políticas indicadas por una organización o entorno de trabajo implementado en OAIS. Son todas las políticas de gestión y están definidas por actividades de administración modo de tarea.	

		Consumidor (Consumer)	Están representados por personas o sistemas cliente que tienen el rol de usuario y consumidor de información preservada. El consumidor interactúa con el sistema haciendo diferentes tipos de solicitudes y obteniendo respuestas, también se define el término comunidad designada, es un tipo de consumidor e incluso puede actuar por momentos con un doble rol tanto de consumidor como productor por el nivel de interacción con el sistema.	
Información del Modelo OAIS	La información dentro del sistema funciona como materia prima, la cual es la principal sustancia que fluye dentro del sistema y por ello debe ser definida desde diferentes funciones a nivel de paquetes de información y descripción de la misma.	**Information Package (IP)**	Los paquetes de información son conectores de información y son de dos tipos: Información de contenido (son todos los datos del objeto) información de preservación (provenir, contextos, referencias, fijación, derechos de acceso). Ambos integran, describes e identifican un objeto o representación de información que son entregados, archivados, diseminados y transmitidos entre productores y consumidores.	
		Submit Information Package (SIP)	Es el paquete de información presentado por el productor al sistema OAIS como inicio del proceso, el que contiene una personalidad de forma y detalle definida por el	

			productor y es validada por el sistema, también poseen información de contenido y descripción de la preservación en un nivel básico.	
		Archival Information Package (AIP)	Contiene un paquete completo de información descriptiva de preservación asociada a la información de contenido. Estos paquetes son más completos que los SIP, ya que contiene información de un objeto con la cantidad y calidad suficiente que garantiza su preservación a largo plazo.	
		Disseminating Information Package (DIP)	Es un paquete de información que surge como respuesta a las solicitudes realizadas por un consumidor, y es entregado como respuesta; puede ser una colección completa de AIPs o solo una parte de ella, y puede tener diversas formas de acuerdo a las necesidades del consumidor.	
		Descriptive Information (DI)	Es un grupo de información descriptiva que se proveen de las acciones de gestión de datos (data management) para facilitar la búsqueda, recuperación y ordena la información empaquetada y solicitada por un consumidor al sistema	

Entidades Funcionales	El modelo OAIS se compone de seis entidades funcionales, las cuales proporcionan diferentes servicios y funciones mediante una interfaz relacionada de actuación en el modelo.	**Preservation Planning (Planificación de Preservación)**	Son actividades de prioridad para el monitoreo de los diferentes entornos de producción, consumidor y gestión mediante diferentes funciones, servicios, normativas y estrategias que garantizan que la información almacenada esta accesible y entendible a largo plazo para la comunidad designada.	• Planificación de preservación de la información • Evaluación del contenido de archivos. • Actualizaciones periódicas. • Migración de soportes para los archivos. • Desarrollo de recomendaciones y normativas. • Reporte y análisis de riesgos. • Desarrollo de planes de migración e implementación de prototipos de software para obtener los resultados esperados.
		Administration (Administración)	Posee una serie de servicios y funciones en las operaciones de un sistema de archivo como son loa acuerdos, negociaciones y envíos; también da mantenimiento a los sistemas de software y hardware, monitorea, actualiza, hace inventarios, migra y reporta el estado del sistema.	
		Ingest (Ingesta)	Esta entidad incluye funciones y servicios de aceptar los SIP de los productores, preparando y asegurando la calidad de los AIP y de que la información descriptiva se establezca en el sistema OAIS como paso previo a su depósito en el almacenamiento de archivos.	

		Data Management (Gestión de Datos)	Esta entidad realiza actividades de mantenimiento en la información descriptiva y administrativa asegurando el acceso de manera continua a los datos depositados en el sistema; las funciones que realiza es administrar, actualizar la base de datos.	
		Archival Storage (Archivo de almacenamiento)	Su función principal es la de almacenar, mantener y recuperar los paquetes de información, en el momento de almacenar su característica es la jerarquizar los paquetes por orden, lleva a cabo revisiones de rutina en los errores de archivos y paquetes lo que permite mantener accesibilidad de manera estable	
		Access (Acceso)	Brinda soporte a los usuarios sobre la localización, existencia, disponibilidad y descripción de la información almacenada en el sistema. También posee actividades de comunicación entre clientes, consultas y respuestas, entrega la información solicitada mediante informes.	
Interacciones		**Queries (Peticiones)**	Dentro del sistema OAIS sus diferentes actividades realizan peticiones de manera interna, y en la entidad acceso es donde hacer peticiones externas ya que son realizadas por los usuarios.	

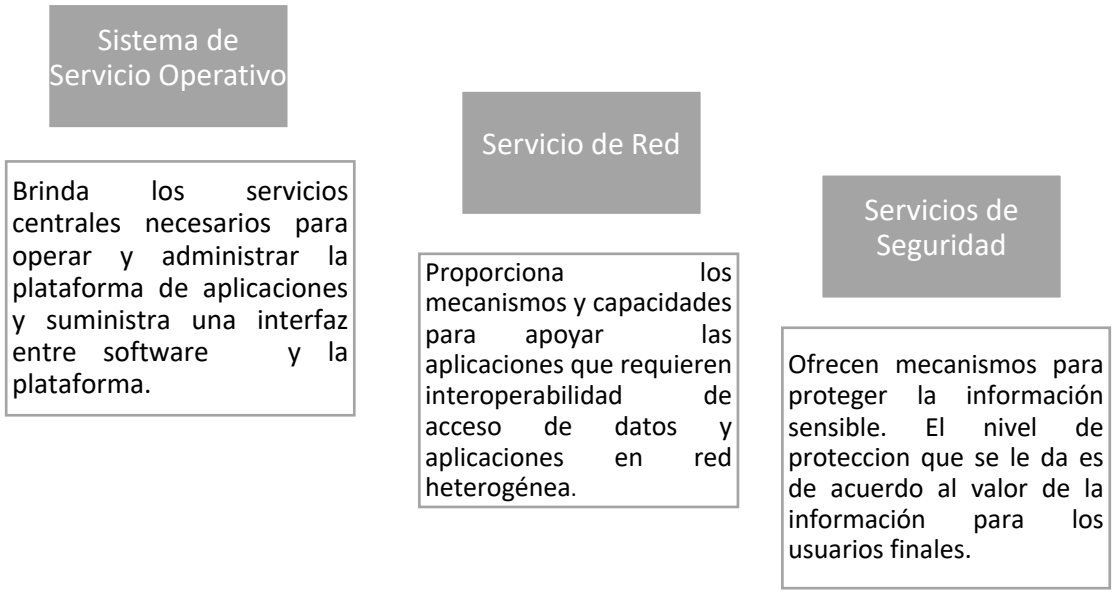
		Queries Responses (Respuesta a peticiones) y orders (ordenes)	Estas peticiones son entrega de información, y las ordenes que se recibe son específicas, objetivas que realizan los usuarios al sistema y en las que obtienen paquetes de informaciones específicas.	

Realizado por: Marilú Torres, 2021

Fuente: David Leíja Román, 2017, p. 43-48

Además de las entidades antes mencionadas también se refiere a los Servicios Comunes que están disponibles en una infraestructura tecnológica. Se considera a estos servicios como otra entidad funcional:

Servicios Comunes usados por el modelo OAIS



Realizado por: Marilú Torres, 2021

Fuente: Claudia Castillo, s. f.p. 23

2.2.5.1.2. Modelo de la Información

Aquí se detalla los tipos de información que se intercambian y gestionan dentro del OAIS, y su modelo define los objetos de información específicos que se emplean para preservar y acceder a la información de un archivo.

El concepto principal para este modelo es **Paquete de Información** que está compuesto por información descriptiva de la preservación, también se relaciona a este término la información de empaquetado que es utilizada para identificar y delimitar la información de contenido y la información de descripción del empaquetado que facilita la búsqueda de la información de contenido. (Claudia Castillo, s. f.p. 23)

Figura 3-2: Estructura del Paquete de Información
Fuente: Claudia Castillo, s. f.p. 23

Este paquete se caracteriza por ser comprensible de manera independiente, esto quiere decir que posee información completa y suficiente para ser interpretada, entendida y utilizada por la comunidad designada (usuarios finales), sin tener que recurrir a un entorno tecnológico o recursos especiales en un momento determinado.

Tabla 7-2: Estructura del Paquete de Información

Estructura del Paquete de Información			
Componentes	***Definición***	***Metadatos***	***Ejemplo***
Información de Contenido	Conjunto de información que es el objetivo principal de la preservación	**Información del objeto de datos de contenido.** Es el objetivo digital o datos (bits) a preservar	Documentos digitales con contenido de texto, audiovisual, sonoro, fotográfico.
		Información de representación asociada. Es utilizada para la interpretación y comprensión del objeto de datos.	Especificaciones técnicas de software y formato digital. Glosarios
Información de descripción de la preservación	Información que es necesario para la preservación adecuada de la información de contenido. Sustenta la confianza, el acceso y el contexto de la información de contenido durante su ciclo de vida.	**Información de referencia** Identifica y describe inequívocamente al documento digital.	Descripción archivística normalizada.
		Información de contexto Documenta la relación del objeto de datos de contenido con otro objeto o con el contexto documental.	Identificadores o referencias a otros documentos o archivos relacionados con la información de contenido.
		Información de Procedencias Historias de la información de contenido, desde su origen o fuente de información.	Pistas de auditoría de la Información de Contenido
		Información de Integridad Documentación de los mecanismos empleados para comprobar la integridad y autenticidad.	Firmas Electrónicas, certificados digitales.
		Información de derechos de acceso Identifica las restricciones de acceso a la información de contenido, incluido el marco legal y el control de acceso.	Condiciones de preservación y uso incluido en los acuerdos de transferencia establecidos entre los productores y el archivo OAIS. Políticas de control de acceso.
Información de Empaquetado	Información que se utiliza para vincular e identificar los componentes de un Paquete de información en un contenedor neutral.	Información de la estructura del formato contenedor del paquete de información. Información del método de empaquetado.	Formato XML. Es el contener más recomendado para la información de empaquetado.
Información descriptiva del empaquetado.	Conjunto de Información que permite la búsqueda, ordenamiento y recuperación de la información del contenido de interés.	Información del paquete de información basada en modelos de metadatos descriptivos que permite la gestión de datos con el fin de apoyar la recuperación y localización de datos.	Instrumentos de acceso y consulta basados en modelos de metadatos descriptivos como: Dublín, CORE, ESE, MODS y EAD.

Fuente: Claudia Castillo, s. f.p. 25

2.2.5.1.3. Propósito del Modelo OAIS

El modelo OAIS establece un conjunto de propósitos, prácticas y recomendaciones como referencia para los diferentes escenarios de trabajo que ayuden a entender, analizar e incentivar la actividad de la preservación a largo plazo de información digital, proporcionando un escenario con terminologías y conceptos donde se describen los procedimientos utilizados en la arquitectura. (David Leíja Román, 2017, p. 41)

2.2.5.1.4. Aplicaciones del Modelo OAIS

Este modelo es aplicable a todo tipo de archivo en estado físico o digital de cualquier organización que sea responsable de mantener toda la información disponible a largo plazo, también se puede aplicar a archivos temporales esto de sebe al cambio continuo de la tecnología este modelo puede ser flexible en su adaptación de conceptos y terminologías teniendo en cuenta las necesidades de preservar la información. (David Leíja Román, 2017, p. 41)

2.2.5.2. Modelo PREDECI

El modelo PREDECI se divide en un conjunto de tres niveles y ocho entidades funcionales, donde se conserva la información de acuerdo al modelo. Este modelo especifica cómo se debe administrar la información y cómo se transmite la información a partir de los datos de la entidad funcional de ingestión para acceder a la entidad funcional. También tiene la responsabilidad de proteger la información al largo plazo para aumentar la aceptabilidad de documentos digitales y garantiza la fidelidad e integridad al largo plazo y responde a un conjunto de responsabilidades especificadas en las leyes y regulaciones basado en el modelo de preservación de OAIS y Conceptos de metadatos. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 20)

Estructura Funcional de PREDECI

Proporciona una vista más detallada de las diferentes entidades funcionales que ayuda en el entendimiento y la implementación de las aplicaciones. Este modelo se divide en 6 entidades funcionales: Ingesta, Área de Archivo, Gestión de Datos, Administración, Planificación y Preservación a su vez especifica como la información debe ser gestionada y trasmitida a partir de datos de ingesta. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 21)

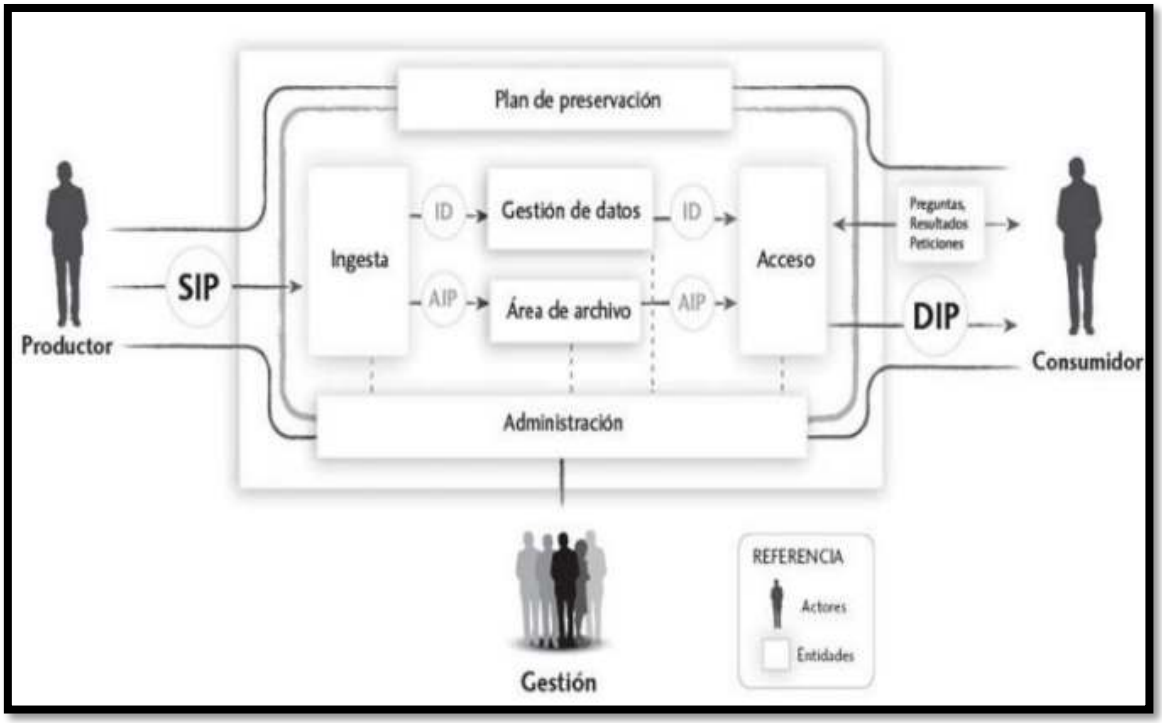


Figura 4-2: Diagrama de la Estructura Funcional de PREDECI
Fuente: Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 21

Tabla 8-2: Entidades Funcionales del Modelo PREDECI

Funciones	***Detalles***
Ingesta	Proporciona la capacidad de almacenamiento para recibir un SIP de un productor, y este se entrega mediante medios de transferencia electrónica al sistema para acceder a los archivos.
Área de Almacenamiento	Esta área permite usar diferentes mecanismos como locales o remotos y para almacenar la información codificada digitalmente, en su función de recepción recibe una solicitud de almacenamiento de datos desde la ingesta AIP los cuales permanecen dentro del archivo.
Gestión de Datos	Se encarga de la integridad de la gestión de la base de datos y proporciona mecanismos de almacenamiento de información de manera descriptiva y describe las propiedades del archivo y sistema.
Administración	Posee las mismas funciones que OAIS con características que los informes contendrán información de las funciones, y la presentación de los formatos y procedimientos de datos deben estar documentados, los envíos y entregas de archivo de datos deben estar identificados por el productor.
Plan de Preservación	Se encarga del desarrollo de estrategias, estándares y evaluaciones de riegos de la infraestructura del sistema,

	proporciona el análisis de riesgos y mitigación para el buen funcionamiento de políticas, normas y procedimientos.
Acceso	Se incluye la legalidad y validación del consumidor.

Realizado por: Marilú Torres, 2021

Fuente: Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 22, 23

Guía de Implementación del Modelo PREDECI

PREDECI consta de un conjunto de tres niveles y ocho entidades funcionales, podemos decir que estas entidades funcionales conservan la información de acuerdo con la información definida en el modelo.

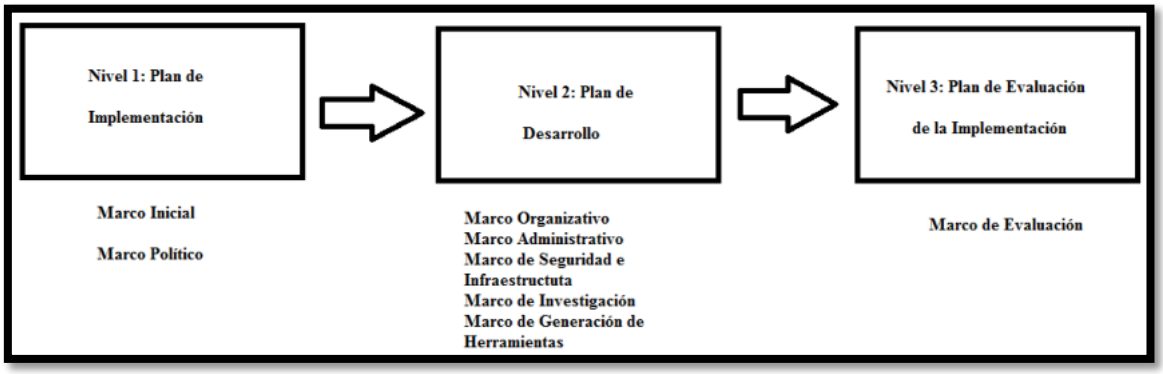


Figura 5-2:Guía de Implementación del Modelo
Fuente: Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 23

Nivel 1: Plan de Implementación

- Marco Inicial: Obtener compromisos de la Administración
- Marco Político: Determinar el estado actual y proponer el estado futuro

Nivel 2: Plan de Desarrollo

a) Marco Organizativo
    - Determinar la Gobernabilidad y viabilidad organizacional.
    - Determinar la estructura del Personal
    - Definir los Objetivos
    - Definición de criterios para objetivos digitales.
    - Definición de responsabilidades para preservación a largo Plazo.
    - Designación del personal para el Área del Departamento de Gestión Documental.
    - Definición de reglas.

- Establecimiento de personal calificado. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 23)

b) Marco Administrativo
    - Definición de Políticas de integridad de los objetos digitales.
    - Definición de Políticas de autenticidad de los objetos digitales.
    - Definición de un plan estratégico para la preservación.
    - Determinación de criterios para aceptación de objetos digitales de productores.
    - Determinación de criterios de usabilidad para os objetos digitales.
    - Determinación de aspectos de administración de datos.
    - Configuración del acceso para la administración.

c) Marco de Seguridad e Infraestructura
    - Determinación de la infraestructura adecuada.
    - Determinación de la infraestructura de seguridad para objetos digitales.

d) Marco de Investigación
    - Configuración de evidencias (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 24)

e) Marco de Generación de Herramientas
    - Creación de la Aplicación
    - Instalación y Configuración

Nivel 3: Plan de Evaluación de la Implementación

a) Marco de Evaluación
    - Evaluación del Estado Final
    - Informe Final
    - Validación de los Resultados. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 25)

2.2.5.3. Modelo PREMIS

PREMIS son las siglas de "PREservation Metadata: Implementation Strategies" que es el nombre de un grupo internacional patrocinado por Online Computer Library Center (OCLC) y Research Libraries Group (RLG) que, como su nombre lo indica, se enfoca en estrategias de implementación de metadatos de preservación en Archivos Digitales. (Marisa Giusti, 2015)

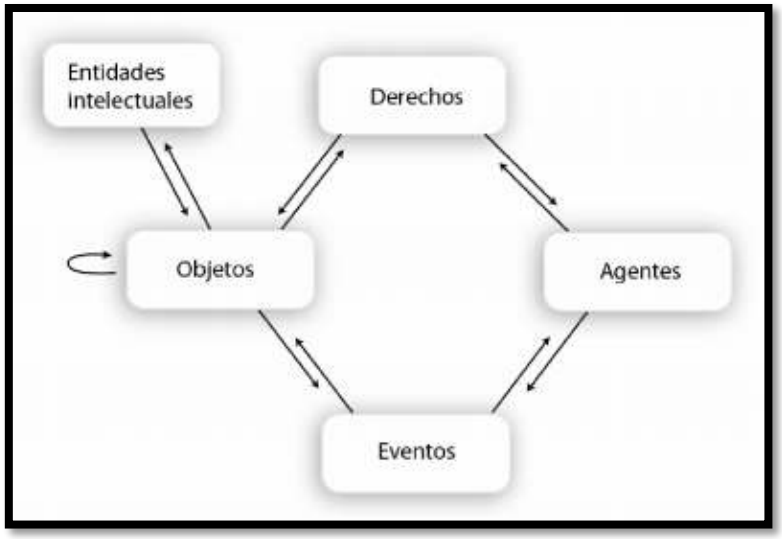


Figura 6-2: Modelo de Datos PREMIS
Fuente: Marisa Giusti, 2015

Se enfoca en el sistema de repositorio y en su gestión, los metadatos PREMIS se centran en el diseño de los repositorios, para su evaluación y para el intercambio de los paquetes de información archivada entre los repositorios de preservación. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 20)

Entidad Intelectual

Es un conjunto de contenidos que se considera como una unidad intelectual individual a los propósitos de gestión y descripción. El diccionario de datos no determina los metadatos descriptivos a vincular a una entidad intelectual, sino que deja abierta a la elección de cualquier formato deseado. (Marisa Giusti, 2015)

Ejemplo:

- Conjunto de contenidos a os que se considera entidad intelectual: Libros, mapas, fotografías, base de datos
- Entidad Intelectual que pueden contener otras entidades intelectuales son sitios web. (Marisa Giusti, 2015)

2.2.5.3.1.1. Objetivos

Unidades discretas de información en forma digital, que se clasifican en tres tipos: archivo (file), representación (representation) y cadenas de bits (bitstream).

- El objeto archivo es tal cual se entiende normalmente, en un archivo PDF de un capítulo de un libro.
- El objeto representación es el conjunto de todos los archivos que se necesitan para representar la entidad Intelectual incluyendo los metadatos estructurales.
- Los objetos cadenas de bits son subconjuntos de archivo con propiedades útiles a la preservación, en el ejemplo del libro el archivo JPEG de la tapa puede tener sus propios identificadores y metadatos.

La información que se puede registrar en los objetos incluye: un identificador, la integridad, el tamaño, información sobre la creación, sobre el entorno, el soporte y la relación con otros objetos y otros tipos de entidades. (Marisa Giusti, 2015)

2.2.5.3.1.2. Eventos

La entidad Eventos agrega información sobre acciones que un agente, o varios, lleva adelante sobre los objetos de los repositorios, por ejemplo: el identificador del acontecimiento (no repetible), el tipo (creación, migración, etc), la fecha de ocurrencia del evento, la descripción y el resultado codificado del acontecimiento, así como los agentes. (Marisa Giusti, 2015)

2.2.5.3.1.3. Agentes

Los Agentes pueden ser personas, organizaciones o aplicaciones de software con actividades o responsabilidades en los eventos. El Diccionario de datos aconseja como información: un identificador único, el nombre del agente y su tipo. (Marisa Giusti, 2015)

2.2.5.3.1.4. Derecho

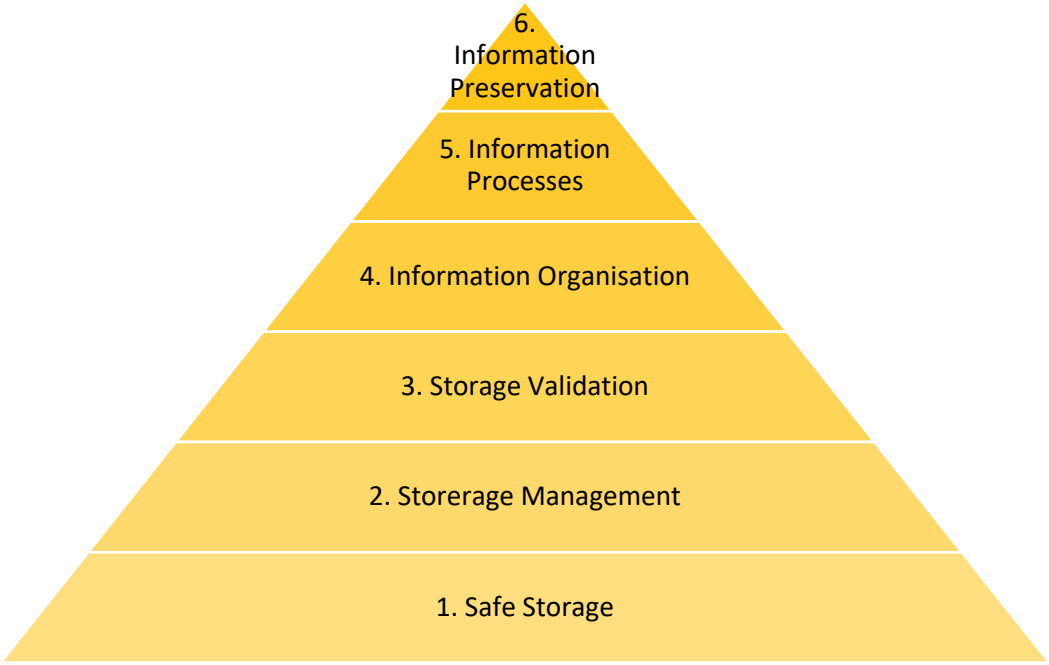
Corresponden a la declaración de uno o varios derechos o permisos pertenecientes a un Objeto que se encuentra en un repositorio y donde queda registrada una gran variedad de información sobre los derechos, desde resúmenes de declaraciones de derecho hasta los permisos y derechos de agentes externos y objetos no depositados en el repositorio. Es la que hace referencia a los derechos o permisos con los que un repositorio tiene que cumplir y que corresponde a las acciones que afectan a los objetos dentro del repositorio. (Marisa Giusti, 2015)

2.2.5.4. Modelo DAMM

DAMM (Digital Archiving Maturity Model) Modelo de Madurez de Archivo Digital este modelo se utiliza para implicar de sofisticación en los procesos, el primero de los cuales debe ser completa antes de pasar a la siguiente, para la preservación digital no tiene sentido tener un sistema de gestión de la información inteligente cuando no se tiene un almacenamiento más seguro. (Rubén Pilco Pilco, 2015, p. 35)

Componentes claves

Consta de tres secciones principales y de 6 capas:



Digital Preservation Maturity Model

Fuente: Rubén Pilco Pilco, 2015, p. 41

- **Almacenamiento Durable**

  Las capas 1 y 3 proporcionan mayores niveles de sofisticación de la seguridad y la seguridad de almacenamiento de los bits, el tiempo que tiene un sistema compatible con el nivel 3 se está seguro de que su información no se perderá y no será manipulado. (Rubén Pilco Pilco, 2015, p. 40)

- **Gestión de la Información**

  En las capas 4 y 5 aseguran que los bits primos conservadas se organizan. Poseen una jerarquía, los metadatos descriptivos y la seguridad poseen un conjunto de herramientas de gran alcance para permitir que suba la gestión, búsqueda, navegación y descargar.

- **Información de Preservación**

  La capa 6 se encarga de retener la información por mas vida útil de la aplicación que lo creo y asegura los formatos de archivos y de información son pertinentes para aplicaciones disponibles en el momento que sea solicitado o requerido lo que es de manera inmediata (Rubén Pilco Pilco, 2015, p. 40)

Tabla 9 -2: Niveles del Modelo DAMM

Niveles	***Tema***	***Definición***	***Característica***
Nivel 1	Almacenamiento Seguro (Safe Storage)	En este nivel se incorpora de manera sencilla el almacenamiento a nivel de bit o de almacenamiento magnético u óptico con un cierto nivel de seguridad de que los bits están protegidos contra fallo de almacenamiento simple. Esto incluye el almacenamiento en discos giratorios protegidos utilizando técnicas RAID, medios ópticos con el almacenamiento a largo plazo y ubicaciones gestionadas, o almacenamiento en cinta para toda la vida.	• Resistencia a amenazas comunes como el daño físico menor.
Nivel 2	Administración de Almacenamiento (Storege Management)	En el nivel 2 se añade la gestión de almacenamiento activo que mueve los bits a la ubicación más adecuada. Se toman decisiones sobre qué bits se encuentra dónde puede ser hecho, la reducción de coste o rendimiento. Los criterios son flexibles para equilibrar todos estos conductores. La información debe ser guardada en al menos dos lugares, por ejemplo, disco y cinta de copia de	• Reglas para mover objetos entre ubicaciones de almacenamiento en función de costes, durabilidad o rendimiento. • Puede ser almacenado en dos lugares. • Las reglas pueden cambiar en cualquier momento para mover la ubicación a lugares diferentes.

		seguridad o varias réplicas de disco.	
Nivel 3	Almacenamiento de Validación (Storage Validation)	En este nivel la sofisticación de almacenamiento final añade objetos múltiples, y realiza comprobación para validar la durabilidad de almacenamiento. La fijeza del objeto se comprueba en el almacenamiento, acceso y en intervalos regulares para confirmar los objetos no han sido alterados. Si se identifica el fracaso de bits, se producirá auto curación de una copia alternativa.	• Las copias de información se realizan en diferentes lugares de almacenamiento. • Sumas de verificación creada para todos los elementos de información en virtud de almacenamiento. • También usa las sumas para comprobar la integridad de la información. • Auto-curarse de copia alternativa si se detecta la corrupción de la información.
Nivel 4	Organización de Información (Information Organisation)	En el primer nivel de gestión de la información incorpora la capacidad de convertir archivos a nivel de bits en bruto, en este nivel se hace un aumento en dramático en la utilidad de a información.	• Información organizada en jerarquías donde se comprende muchos archivos, objetos de información. • Información etiquetada con metadatos donde existe una descripción, historia y contexto. • Herramientas para subir nueva información. • Se crea modelo de seguridad para limitar el acceso a la información. • Se crea permisos que editan los metadatos, modifican la jerarquía y elimina el contenido.
Nivel 5	Procesos de Información (Information Processes)	Aquí se añade procesos de negociación de manera eficiente y flexible para automatizar las actividades de la gestión de información. También incluyen capacidades de alto rendimiento y la integración con los sistemas de gestión de identidad de terceros.	• Herramientas como son los flujos de trabajo para permitir la automatización de procesos de negociación. • Se realizan interfaces programador que permite la extensión del sistema. • Integración con las ubicaciones de origen y eliminación de contenido.
			• Identifica los formatos de archivos y objetos conceptuales.

Nivel 6	Información de Preservación (Information Preservation)	La información digital debe ser utilizada por la persona que lo desee. Cuando se retine información por más de 10 años su uso se hace imposible para evitar esto se debe incorporar herramientas para la preservación de la información y poder dar soluciona este problema.	• Extrae las características de los objetos para la validación. • Identifica los formatos de archivos que están en riegos y con necesidad de atención. • Realiza la migración de pérdida a los nuevos archivos. • Realiza la migración con pérdida de formato de presentación en calidad adecuada para la difusión. • Mantiene la información digital original para presentaciones creadas mas tarde. • Crea nuevas herramientas para mantener la información de preservación activa.

Realizado por: Marilú Torres, 2021

Fuente: Rubén Pilco Pilco, 2015, p. 41- 44

Tabla 10-2: Resumen de los Modelos de Preservación Digital

Modelos	**Características**
OAIS (ISO 14721:2003)	❖ Es el modelo base que su emplea en la conservación de archivos digitales. ❖ Este modelo posee vigilancia tecnológica en la preservación digital y están e ubicados en una base de datos de los cuales no pueden ser alterados, modificados o perdidos.
PREMIS (Caplan, 2009)	❖ Se utiliza en la preservación de Archivos Digitales como estrategia para su implementación. ❖ PREMIS posee metadatos que actúan solo en la preservación y no poseen vinculación con los metadatos de acceso, recuperación de información y mucho menos con la información sobre derechos.
PREDECI	❖ Este modelo especifica cómo se debe administrar la información y cómo se transmite la información. ❖ Tiene la responsabilidad de proteger la información al largo plazo para aumentar la aceptabilidad de documentos digitales y garantiza la fidelidad e integridad.
DAMM (Preservica, 2013)	❖ Este modelo utiliza capas de sofisticación en los diferentes procesos. ❖ Se debe tener un sistema de gestión de la información con almacenamiento seguro.

Realizado por: Marilú Torres, 2021

2.2.6. Repositorios Digitales

En este sentido práctico y funcional podríamos decir que repositorio digital es un sistema informático integral que almacena objetos digitales completos (documentos, audio, videos, fotografías, bases de datos, etc.) de manera ordenada y accesible. Este puede alojarse vía un servidor web o de un servidor local. Puede ser de acceso abierto o cerrado mediante un software que gestiona la ingesta, clasificación y mantenimiento de objetos digitales. (David Leíja Román, 2017, p. 49)

Los repositorios digitales son sistemas de red formado por hardware, software, data y procedimientos que poseen objetos digitales, metadatos, asegurando la identificación con un identificador único, ofrece función de gestión, preservación y archivos de los objetos, proporciona un acceso fácil y controlado, sistemas de seguridad de los objetos y metadatos que sean sostenibles en el tiempo. También perite la recuperación, reutilización y preservación de los resultados de investigación, además de la difusión y visibilidad de la producción garantizando de manera efectiva el avance de la ciencia. (Beatriz Peña, 2015, p. 34)

2.2.6.1. Características de Repositorios Digitales

Poseen 4 características fundamentales:

- Contiene objetos digitales
- Contiene metadatos
- Asegura la identificación persistente del objeto mediante un identificador único persistente.
- Funciones de gestión, archivo y prese5vación de los objetos.
- Proporciona un acceso fácil, controlado y estandarizado a los objetos.
- Ofrece los sistemas adecuados de seguridad para los objetos y los metadatos.
- Sostenible en el tiempo. (Flavio Cerón Romo et al., 2017, p. 27)

2.2.6.2. Clases de Repositorios Digitales

Tabla 11-2: Clases de Repositorios Digitales

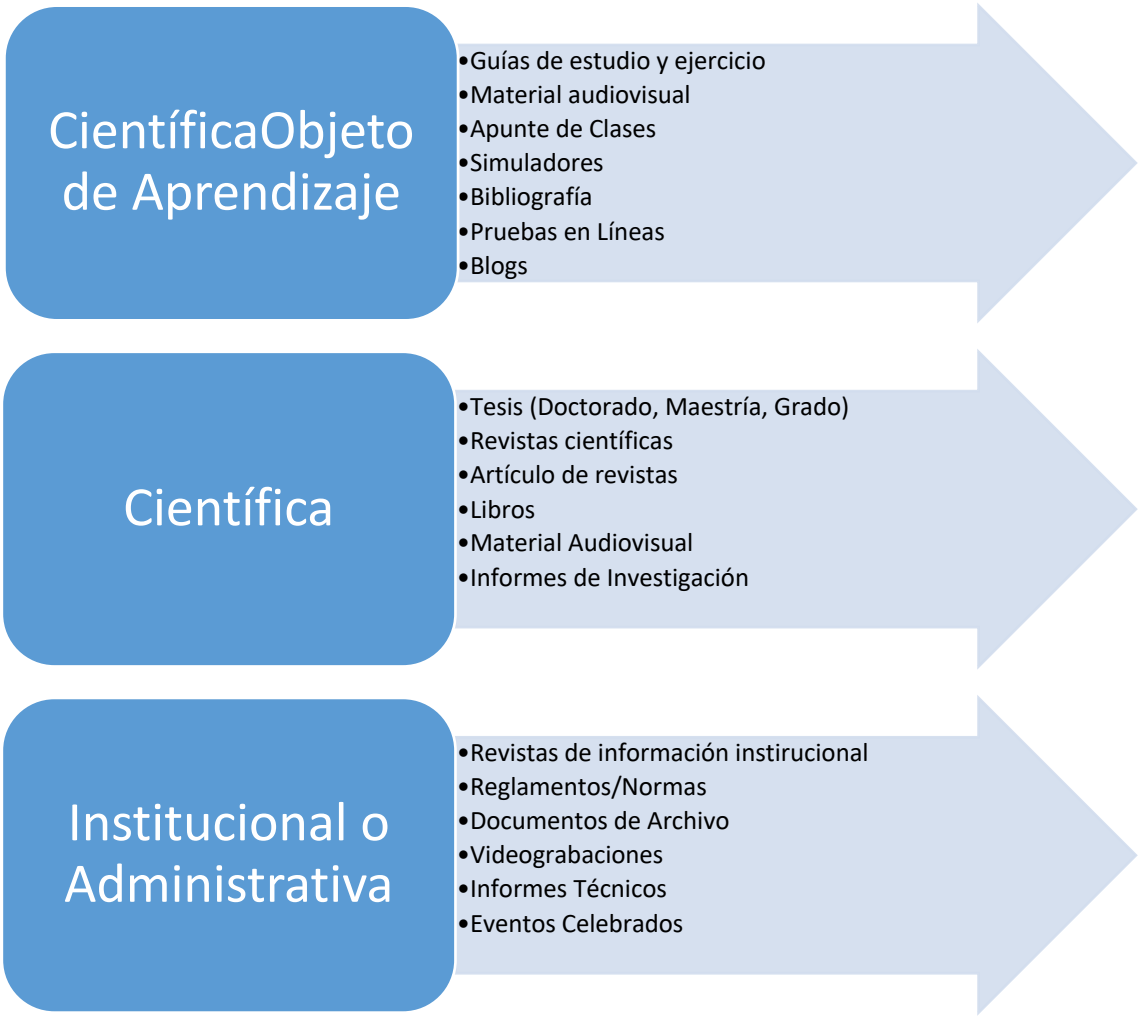
Repositorio Digital	***Definición***
Repositorios Institucionales	Almacenan, preservan, diseminan y dan acceso a la producción intelectual de los miembros de la institución. Contienen solamente la producción intelectual, científica (artículos, tesis, paper, datos, etc.).
Repositorios Temáticos	Preservan y dan acceso a contenidos de una disciplina o tema específico. Son creados y mantenidos por instituciones académicas, investigación u organismos gubernamentales.
Repositorios de Datos Básicos	Almacenan y preservar datos científicos generados en el proceso de investigación. Son repositorios independientes pero también pueden ser integrados a los repositorios institucionales.
Repositorio Huérfanos	Están establecidos para el archivo de trabajo de autores que no tienen acceso a otro repositorio (institucional o temático). Son establecidos a nivel nacional.
Agregado/ Recolectores	Recolectan los contenidos de repositorios institucionales y temáticos/ disciplinares, estas agregaciones pueden ser geográficas (regional o nacional), área temática o tipo de documentos (Tesis, paper, etc.).

Realizado por: Marilú Torres, 2021

Fuente: Flavio Cerón Romo et al., 2017, p. 27, 28

2.2.6.3. Tipos de Documentos en los Repositorios Digitales

Los repositorios digitales pueden contener distintos tipos de documentos o información: científica, institucional, administrativa y objetos de aprendizaje.



Realizado por: Marilú Torres, 2021

Fuente: Flavio Cerón Romo et al., 2017, p. 28

2.2.7. Evaluación de Preservación Digital en Repositorios Digitales

Se detalla los parámetros de un repositorio apropiado para modelo de preservación digital, junto con las aportaciones, "Grupo de trabajo, autores de Catálogo de Criterios para Repositorios Digitales Confiables, establecieron condiciones, establecieron condiciones para crear repositorios y archivos digitales seguros, auditables; luego, escogieron diez requisitos que los repositorios digitales deberían cumplir para garantizar los resultados de su funcionalidad en un largo tiempo, a saber". (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 25)

- Responsabilidad con los documentos digitales
- Legalidad
- Eficiencia y Eficacia con las políticas.

- Organización
- Infraestructura técnica adecuada
- Integridad, Autenticidad y usabilidad en la conversión del objeto digital
- Adquisición
- Gestión de Metadatos
- Planificación y Actuación
- Difusión (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 25)

Existe modelos de evaluación TRAC, DRAMBORA y NESTOR que usan el modelo de referencia OAIS, que tienen el mismo objetivo de establecer parámetros para medir el cumplimiento de todas sus funcionalidades.

2.2.7.1. DRAMBORA

DRAMBORA (Digital Repositorio Auditoría método basado en la evaluación de riesgos) es una herramienta de evaluación de repositorios basado en papel el cual permite la comprensión de los documentos archivados y los riesgos que estos enfrentan, presentando términos de probabilidad y el impacto potencial. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 25)

Beneficios del DRAMBORA

Ayuda a fortalecer la confianza de los usuarios y del personal, aumentando la eficiencia en la colección de archivos digitales valiosos en situación de riesgo.

2.2.7.2. NESTOR

Los recursos digitales han emprendido esfuerzos para diseñar un catálogo de criterios para repositorios digitales de confianza donde la red de experiencia es la base primordial y su objetivo principal es introducir criterios de evaluación de repositorios digitales a largo plazo. Los criterios de catálogo NESTOR se han formulado a nivel abstracto y cada criterio se enriquece con explicaciones detalladas y ejemplos concretos que se agrupan en secciones tituladas Organización marco, objeto de Gestión e Infraestructura y Seguridad, Integridad de la Información. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 26)

Principios Básicos

- **Adecuación. -** La evaluación se basa en los objetivos y tareas del repositorio digital a largo plazo.
- **Cuantificación. -** Se lo realiza en algunos casos en relación a los aspectos de largo plazo, no existe características medibles, por lo cual se debe confiar en los indicadores.
- **Documentación. –** Los objetivos, especificaciones e implementación del repositorio digital deben ser documentados, de esta manera se puede evaluar el estado del desarrolla a nivel interno.
- **Transparencia.** - esto se logra mediante las publicaciones de las partes acertadas de la documentación, lo que permite medir el grado de confiabilidad por los usuarios. Se establece una confianza entre las partes interesadas para la evaluación de la calidad del repositorio digital. (Rubén Pilco Pilco, 2015, pp. 84, 85)

También es utilizado para la evaluación de los niveles de importancia en el desarrollo del proyecto de investigación y está dirigido a organizaciones de memoria de archivos, bibliotecas, museos proporcionando una guía de cómo está actualmente la institución en la administración de archivos.

Tabla 12-2: Dimensiones del Catálogo Néstor

Nombre	***Detalles***
Repositorio Digital y sus Objetivos	• El repositorio digital ha desarrollado criterios para la selección de sus objetivos. • El repositorio digital asume la responsabilidad de la conservación de la información a largo plazo. • El repositorio digital ha defino a la comunidad designada.
Comunidad Designada y el uso correcto de información	• El repositorio digital garantiza que la comunidad designada puede acceder a los objetivos digitales. • El repositorio digital garantiza que la comunidad designada puede interpretar los objetivos digitales.
Normas Legales	• Contratos legales entre los productores de información y el repositorio digital. • El repositorio digital actúa sobre la base de normas legales. • El repositorio digital actúa sobre la base de los requisitos legales.
	• Se asegura la financiación adecuada del repositorio digital.

Forma de organizar de manera adecuada el repositorio digital.	• Se cuenta con el personal adecuado. • Se desarrolla estructuras organizadas de manera apropiada para el repositorio digital. • El repositorio digital se involucra en la planificación a largo plazo. • Existen tareas de conservación y están garantizadas en la existencia del repositorio digital.
Gestión de Calidad	• Definir todas los procesos y responsabilidades. • El repositorio digital documenta todos sus elementos en base a procesos antes definidos. • El repositorio digital reacciona ante cambios sustanciales.

Fuente: Marilú Torres, 2021
Fuente: Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 27,28

2.2.7.3. TRAC

TRAC (Trusted Repositories Audit & Certification) se encarga de realizar auditorías internas para evaluar que los repositorios digitales sean confiables y capaces de almacenar de manera fiable la migración, y crea una estructura que soportar la certificación externa del repositorio digital.

Términos Generales del TRAC

- Provee de herramientas para la evaluación, auditoria y la certificación potencial de repositorios digitales.
- Determina requisitos de documentación para la auditoria
- Delimita procesos para la certificación
- Establece metodologías apropiadas para determinar la solidez y sostenibilidad de los repositorios digitales. (Mayra Ausay Espinoza & Wilmer Valle Padilla, 2019, p. 26)

2.3. Norma ISO/IEC 27001

2.3.1. Seguridad Informática

Es fundamental saber que recursos de la compañía o institución necesita protección y así poder controlar el acceso al sistema mediante el internet, en la actualidad los usuarios pueden acceder al sistema de información casi desde cualquier lugar. (Remolina Becerra, 2019, p. 12)

Los riesgos, en términos de seguridad, se caracterizan por lo general mediante la siguiente ecuación.

RIESGO= (AMENAZA * VULNERABILIDAD) / CONTRAMEDIDA

La seguridad de la información es un agregado de medidas preventivas, con el fin de salvaguardar y proteger la información bajo la confidencialidad, disponibilidad e integridad, en este sentido la información se puede presentar en diferentes características; no solamente en los medios electrónicos, sino también en los medios físicos. (Jonathan Guarnizo & Edward Prieto, 2016, p. 18)

En la actualidad la información se ha convertido en el activo más valioso para las compañías, instituciones, organizaciones donde se ejecutan metodologías para proteger los registros y mantener una infraestructura adecuada para la custodia y salvaguardar la información.

- **Integridad:** Esta garantiza la modificación, manipulación, borrado y almacenamiento de archivos solo para el personal autorizado de una manera controlada, provee metodologías de seguridad por niveles.
- **Disponibilidad:** Es la capacidad del sistema de información para mantener el acceso en cualquier instante de tiempo, por lo tanto, se controla los intentos de eliminar archivos o modificar registros por medio de la identificación de usuario y clave de acceso.
- **Confidencialidad:** Provee las garantías para identificar los usuarios que acceden al sistema de información, identificando la hora y fecha mediante controles adecuado e implementados. (Jonathan Guarnizo & Edward Prieto, 2016, p. 18)

2.3.2. Serie ISO 27000

A continuación, se hará una breve explicación de los estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Este estándar contiene las mejores prácticas en seguridad de la información para el desarrollo, implementación y mantener los Sistemas de Gestión de la Seguridad de la Información (SGSI). (Luis Remolina Becerra, 2019, p. 20)

La implantación de una ISO 27000 en una organización permite proteger la información de ésta de la forma más fiable posible. Sus principales objetivos son:

1. Preservar la confidencialidad de los datos de la empresa
2. Conservar la integridad de estos datos

3. Hacer que la información protegida se encuentre disponible. (Jonathan Guarnizo & Edward Prieto, 2016, p. 25)

- **ISO/IEC 27000**: Contiene la descripción general y el vocabulario a ser empleado, se utiliza para tener un entendimiento más claro de la serie y la relación entre los documentos.
- **ISO/IEC 27001**: Las normas es certificable y contiene los requisitos para la implantación del Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27002**: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en la seguridad de la información y están organizados en 11 dominios, 39 objetivos de control y 133 controles.
- **ISO/IEC 27003**: Es la gui de implementación de un SGSI e información acerca del uso del ciclo Deming (PDCA), el propósito es orientar hacia una buena implementación efectiva del modelo de seguridad.
- **ISO/IEC 27005**: Establece las directrices para la Gestión del riesgo en la seguridad de la información.
- **ISO /IEC 27034:** Es una guía de seguridad en aplicaciones.

2.3.3. Norma ISO/IEC 27001

Es la norma que detalla lineamientos de seguridad de la información, los que permite implementar la gestión de seguridad de la información de cualquier empresa, organización o institución y mejora de manera continua la seguridad física y lógica de la información, ayuda a proteger la información de posibles robos, daños. (Kelly Bermúdez & Edber Bailón , 2015, p. 10)

Los objetivos están directamente ligados a la seguridad de procesos organizativos, procesos de producción, al ciclo de vida de la información y obviamente, al cumplimiento de la legislación vigente. (Tania Guachi Aucapiña, 2012, p. 25)

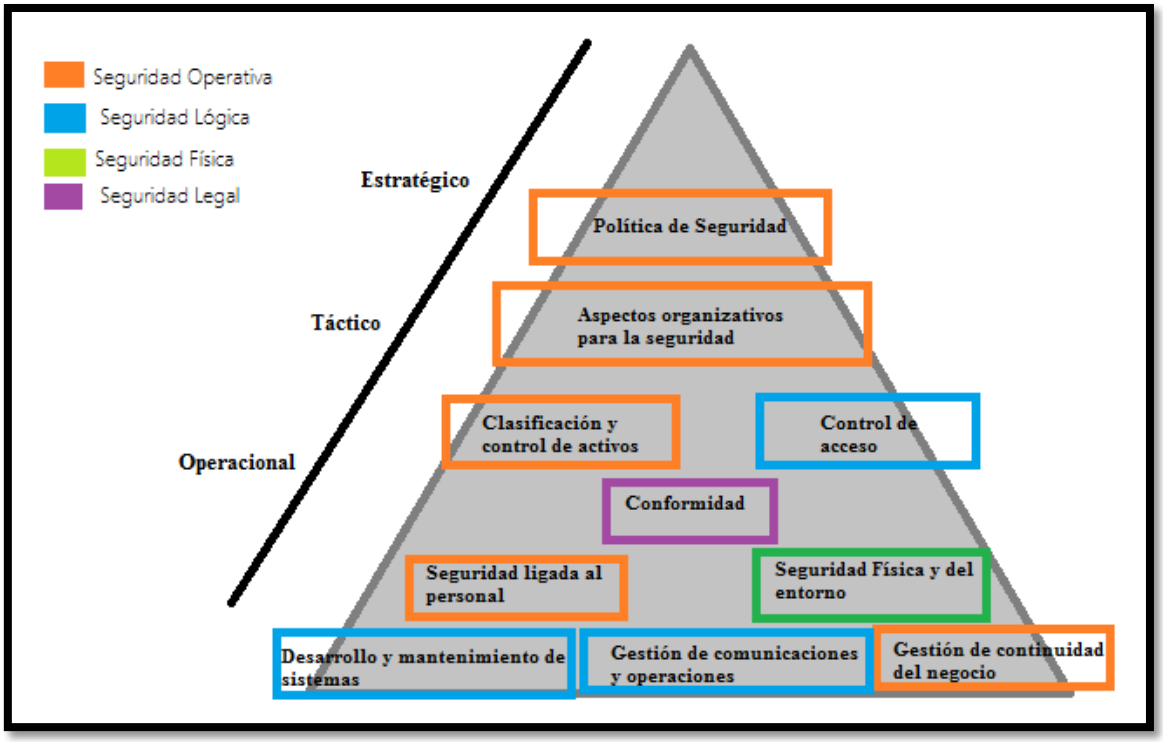


Figura 7-2: Dominios de la Norma ISO/IEC 27001
Fuente: Tania Guachi Aucapiña, 2012, p. 25

La norma ISO/IEC 27001 se divide en 11 secciones, las secciones 0 a 3 con introducidas y opcionales en la implementación, 4 a 10 son obligatorias para la implementación.

Tabla 13-2: Secciones de la Norma ISO/IEC 27001

	Detalle	***Establece***
Sección 0	**Introducción**	El modelo PHVA se lo considera como el Sistema de Gestión de Seguridad de la Información (SGSI)
Sección 1	**Alcance**	ES obligatorio y necesario el cumplimiento de los requisitos establecidos entre los capítulos cuatro y diez de dichos documentos, para obtener una aprobación de cumplimiento.
Sección 2	**Referencias Normativas**	Es la referencia normativa obligatoria y única, que se incluyen todos los nuevos términos y definidos.
Sección 3	**Términos y Definiciones**	Contiene una sola guía de termino y definiciones
Sección 4	**Contexto de la Organización**	Permite identificar todos los problemas externos e internos que se encuentran alrededor de la organización.
Sección 5	**Liderazgo**	Políticas Organizaciones de los roles

Sección 6	**Planeación**	Como abordar riesgos y oportunidades
Sección 7	**Soporte**	Implementación y mejora del SISG a través de los recursos, personal competente, conciencia y comunicación de todas las partes interesadas. Planificación y control operacional
Sección 8	**Operación**	Evaluación de los riesgos de la seguridad de la información
Sección 9	**Evaluación del desempeño**	Realiza la identificación, medición de la eficiencia y el desempeño que realiza SGSI mediante auditorías internas.
Sección 10	**Mejora**	Su elemento principal son las no conformidades identificadas las que deben ser contabilizadas y compradas con las acciones correctivas para asegurar que no se repitan y se tomen las acciones correctivas de manera efectiva

Fuente: Julio Nacipucha Cumbe, 2019, p. 37

En la actualidad la norma ISO/IEC 27001 está formada de 14 controles esto se da por la fusión, exclusión e incorporación de nuevos controles de seguridad. Dentro de cada sección se determina los objetos de controles para la seguridad de la información. El número total de controles suma 114 entre todas las secciones, siendo 14 dominios.

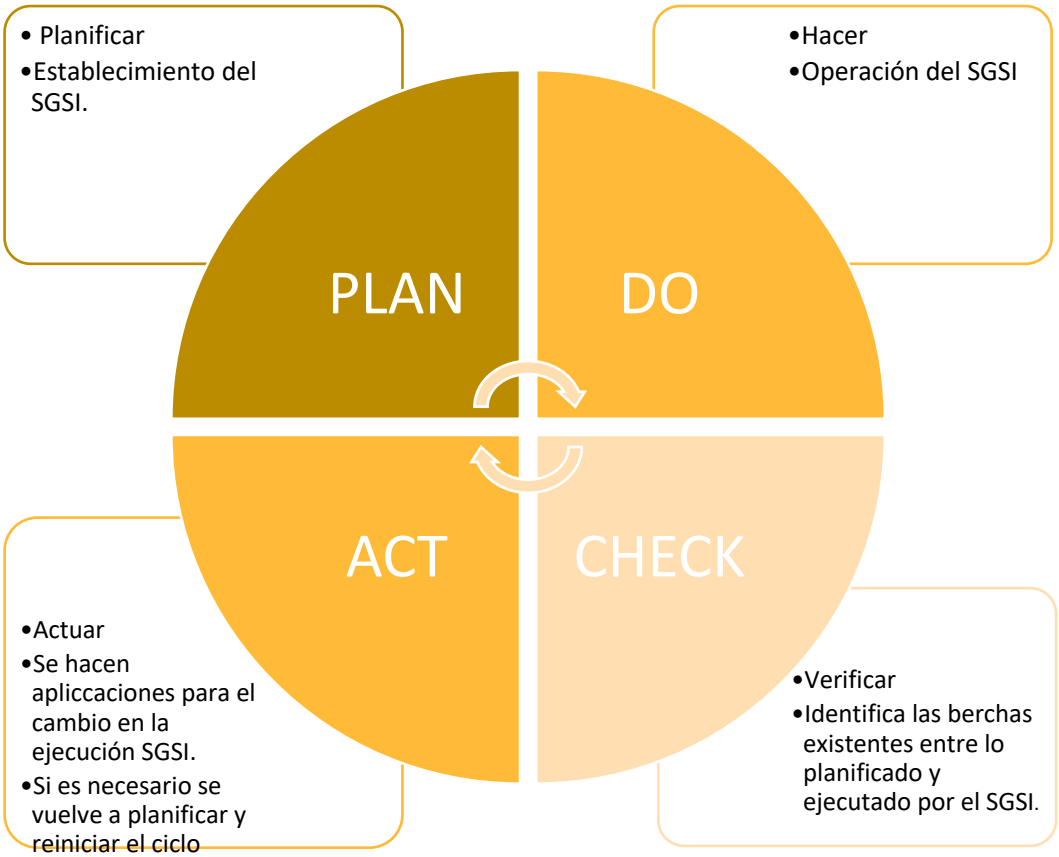
Tabla 14-2: Normas ISO/IEC 27001 Objetivos de Control

NORMA ISO/IEC 27001 OBJETIVOS DE CONTROL	
Política de Seguridad de la Información	Comunicación con los clientes. Políticas de Seguridad no se le puede considerar como una descripción técnica de mecanismos, ni especificación legal.
Organización de la Seguridad de la Información	Establece la administración del resguardo de los datos de la organización como parte fundamental de los objetivos y actividades. Se justifica la importancia de los recursos y la correlación de la seguridad y se determina el responsable de ejercer los correctivos o sanciones.
Seguridad de los Recursos Humanos	Se debe educar e informar al personal sobre las medidas de seguridad es implementada o diseñadas.
Gestión de Activos	La organización debe tener conocimiento de todos los activos que forma parte de la administración de riesgos los que son

	clasificados de acuerdo con la criticidad y sensibilidad de la información.
Control de Acceso	Cada usuario posee su clave de acceso o ingreso para acceder a los recursos de la organización. Para evitar el acceso no autorizado se implementará procedimientos formales de manera escrita.
Criptografía	Se garantiza un uso adecuado y eficaz de la criptografía para resguardar la confidencialidad, autenticidad y la integridad de la información en todo su aspecto.
Seguridad Física y Medioambiental	La primera barrera que debe tener el usuario es no poder acceder a servidores, switch, etc. Las seguridades pueden ser lógicas o físicas, cuando el acceso a la organización este correctamente protegido, así como la información.
Gestión de las comunicaciones y operaciones	Su objetivo es la correcta operación de la información, se debe documentar todos los procedimientos y deben estar disponible para los usuarios.
Adquisición, desarrollo y mantenimiento de los sistemas de operaciones	Se hace un análisis de los requerimientos que están a cargo de los sistemas de información, estos requerimientos deben ser documentados.
Relaciones con Proveedores	Se analiza la implementación de acuerdos para el monitoreo y su cumplimiento con los estándares, y maneja las modificaciones que se puede realizar.
Gestión de incidentes en la Seguridad de la Información	Se hace una metodología de manera eficiente para la definición, generación, monitorización y seguimiento de reportes. Se establece los procedimientos que describe los pasos, acciones, responsabilidades, funciones y medidas de manera concreta. Se necesita personal adecuado.
Gestión de Continuidad del negocio	Son las actividades que reaccionan la interrupción de actividades del negocio y protege sus procesos ante desastres o fallas del sistema.
Marco Legal y buenas practicas	Esta limitado por las leyes de cada empresa, organización, institución de cada país.

Fuente: Julio Nacipucha Cumbe, 2019, p. 38-42

La norma ISO/IEC 27001 promueve la adopción del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización, institución o empresa, así también adopta el modelo de proceso Planear-hacer-chequear-actuar (PDCA), el cual se puede aplicar a todos los procesos del Sistema de Gestión de Seguridad de la Información. (Tania Guachi Aucapiña, 2012, p. 27)



Modelo PDCA con relación al SGSI

Fuente: Julio Nacipucha Cumbe, 2019, p. 43

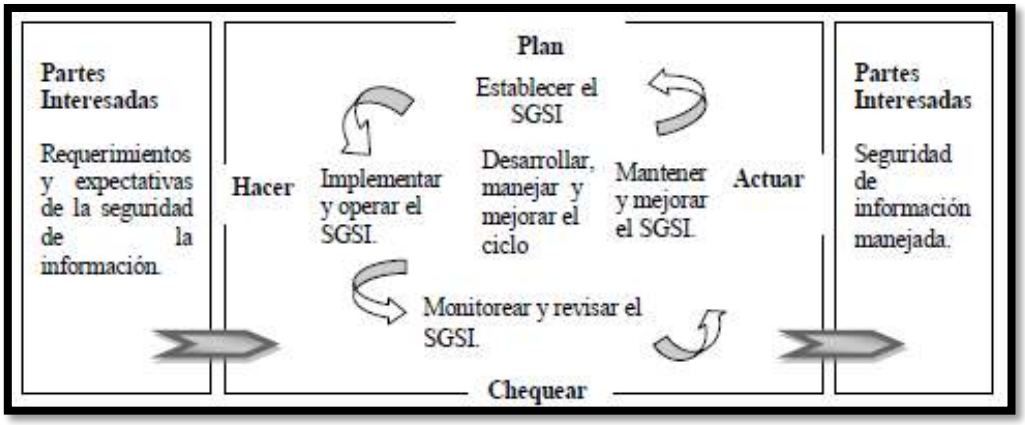


Figura 8-2: Modelo PDCA aplicado a los procesos SGSI
Fuente: Tania Guachi Aucapiña, 2012, p. 28

Tabla 15-2: Secciones de Norma en Relación a la Fase PHVA

Fase PHAVA	*Secciones ISO 27001*
Planear: se establecen los objetivos y actividades del proceso Deming. Se determina el alcance de los requerimientos de la organización.	• **Sección 4:** se realiza un análisis de los problemas internos y externos de la organización, con la finalidad de incorporar las necesidades y expectativas entre las partes interesadas. • **Sección 5:** se est6ablecen los compromisos y responsabilidades por parte de la gerencia. Su principal función son las políticas, responsabilidades y roles de manera pertinente. • **Sección 6:** se establecen como enfrentar los riegos y oportunidades. • **Sección 7**: implementación y mejora mediante los recursos, competencias, concienciación y comunicación de las partes interesadas.
Hacer: Las actividades dentro de la operación Deming facilita la operatividad del Sistema de Gestión de la Información.	• **Sección 8:** se define todos los elementos para la planificación de las evaluaciones y manejo de los riesgos de la seguridad de la información.
Verificar: Se puede identificar las brechas entre lo planeado y le ejecutado en el Sistema de Gestión de la Información.	• **Sección 9:** se define los requerimientos para realizar la identificación, medición de la eficiencia y el desempeño del Sistema de Gestión de la Seguridad de la Información, implementado por auditorías internas y externas.
Actuar: Las actividades establecidas en el ciclo Deming permite hacer cambio en el SGSI, para lo cual es necesario volver a planear y reiniciar el ciclo.	• **Sección 10:** no se debe conformar con lo que sucede para lo cual se debe contabilizar y comparar con las acciones correctivas para dar solución.

Fuente: Julio Nacipucha Cumbe, 2019, p. 44

Beneficios

- Mejora el conocimiento de los sistemas de información, sus problemas y medios de protección.
- Protección de la Información y cumplimientos legales
- Mejora la confianza de clientes al aumentar las garantías de calidad, confidencialidad y disponibilidad.
- Reducción de costos (económicos e imagen) vinculados a incidencias que afecten el tratamiento de la información.
- Establecimiento de una metodología de gestión de la seguridad de la información clara y bien estructurada.
- Riesgos y sus respectivos controles son revisados constantemente.
- Auditorías externas e internas permiten identificar posibles debilidades del sistema. (Tania Guachi Aucapiña, 2012, p. 28)

2.3.3.1. Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información (SGSI) y en inglés (Information Security Management System) sobre este se construye la norma ISO 27001, se realiza un proceso sistemático, documentado y conocido por todos los miembros de la organización, también se considera a proveedores y usuarios (clientes) donde se realiza un enfoque de gestión de riesgos y constituye un Sistema de Gestión da Información. (Julio Nacipucha Cumbe, 2019, p. 45)

La meta del sistema de gestión de la seguridad de la información es asegurar que los riegos de la seguridad sean asumidos, conocidos, gestionados y reducidos por la organización de una manera estructurada, sistemática, documentada, repetible, eficiente y adaptada a los cambios que se pueden generar por los riesgos. (Julio Nacipucha Cumbe, 2019, p. 45)

Los sistemas de información de las organizaciones están expuestos a diferentes amenazas que son aprovechadas por las vulnerabilidades existentes que afectan los activos de diferentes maneras como: fraude, espionaje, sabotaje, vandalismos, incidentes de manera voluntaria o involuntaria por miembros de la organización, amenazas naturales o fallas técnicas.

Figura 9-2: Riesgos a los que se exponen los activos de la organización
Fuente: Julio Nacipucha Cumbe, 2019, p. 46

Fundamentos para la implementación de un SGSI

Su principal función es conocer el contexto de la organización, es decir evaluar los riesgos y ver los diferentes niveles que se le puede dar para que se pueda corregir y gestionar de manera eficiente. Siendo fundamentales los principios de un SGSI:

- Comprender y analizar a la organización en todo su contexto y ver los elementos primordiales que pueden afectar los objetivos del SGSI.
- Conocer todas las necesidades de la parte interesada en relación a la aplicación del SGSI.
- Se realiza las asignaciones de responsabilidad y liderazgo para la seguridad de la información.
- Preparación, formación y concienciación de manera constante para la seguridad de la información.
- Compromiso y liderazgo de la dirección.
- Realizar los test de riesgos para determinar el estado actual de la organización y las estrategias que se emplean en la transferencia, asumir y reducir el riego mediante niveles de aceptación impuestos por la dirección.

- ❖ La seguridad de la información debe ser considerado como elemento esencial.
- ❖ La prevención activa y detección de incidentes de seguridad de la información.
- ❖ Se debe hacer evaluaciones de manera regular en la seguridad de la información y los cambios que se deben implementar de manera apropiada. (Julio Nacipucha Cumbe, 2019, p. 47)

Se debe hacer la identificación de los requisitos para la seguridad de la información iniciando de un contexto global basado en los objetivos generales de la organización, el tamaño, la estrategia de negocio y la posible distribución geográfica en la que se encuentre. Para el establecimiento, control, mantenimiento, y mejora de un SGSI, necesita llevar a cabo los siguientes pasos:

Se debe identificar los activos de información y sus requisitos de seguridad asociados a su valor.

- ❖ Las necesidades del negocio para el procesamiento y almacenamiento de información.
- ❖ Requisitos legales, reglamentos.
- ❖ Necesidades principales de las partes interesadas.
- ❖ Verificar y optimizar la eficacia de controles de seguridad de los activos de información de la organización. (Julio Nacipucha Cumbe, 2019, p. 48)

2.3.3.2. Beneficios de la Norma ISO/IEC 27001

Su principal beneficio es la disminución de riegos de vulnerabilidad en los sistemas informáticos y de la información en general que es manejada por personal de la empresa, organización o institución, además mejora los servicios y procesos prestados, teniendo una mejora en la organización de procesos, aumento de competitividad debido a que se demuestra el interés de salvaguardar la integridad, confidencialidad y disponibilidad de la información. (Kelly Bermúdez &Edber Bailón, 2015, p. 10)

2.3.3.3. Dominios de Seguridad de la ISO/IEC 27001

- Política de Seguridad
- Gestión de Activos
- Seguridad Física y del Entorno
- Control de Acceso
- Organización de la Seguridad
- Cumplimiento

- Gestión de la continuidad de los negocios
- Adquisición, Desarrollo y Mantenimiento de los Sistemas
- Seguridad de los Recursos Humanos
- Gestión de Incidentes de Seguridad de la Información
- Gestión de Comunicaciones y Operaciones

2.4. Seguridad y almacenamiento de la información

La Seguridad de la Información permite mantener y garantizar la integridad, confidencialidad y disponibilidad de la información, se basa en políticas, controles y medidas que abarcan lo preventivo y lo reactivo. La Seguridad Informática, es la seguridad específica aplicada a todos los medios electrónicos que contengan información; entonces cualquier desarrollo humano que se base en componentes electrónicos, de software y la interacción con estos, está abarcado por la seguridad informática.

2.4.1. Sistemas informáticos para el resguardo de la información

Debido al evento de fallo que se pueda presentar en los dispositivos de almacenamiento masivo de información, es importante contar con una copia de seguridad de la información, ya que la probabilidad de que dos dispositivos fallen de manera simultánea es menos probable.

2.4.2. Backup

El llamado "backup", "copia de seguridad" o "copia de respaldo", en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Estas copias son útiles ante distintos eventos como: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales.

2.4.2.1. Medios de Respaldo

Cuando se planifica una estrategia de respaldo o de copias de seguridad lo primordial es considerar el soporte que se utilizará para tal efecto. Esta decisión depende de varias variables, tales como: frecuencia, volumen de datos a copiar, la frecuencia, disponibilidad de la copia y el tiempo en que toma el sistema en ser recuperado.

2.4.2.2. Utilitarios nativos GNU/Linux.

Respecto a las distribuciones Linux, estas cuentan con utilidades de copia de seguridad nativas que se las puede utilizar directamente para realizar backups, o que son utilizadas por otras herramientas más avanzadas de respaldo de información, a continuación las más importantes:

- **Rsync:** Es una herramienta o programa open-source para sistemas de tipo Unix y Windows que se puede usar para sincronizar dos carpetas incluso si están en equipos diferentes dentro de una red. Mediante una técnica de delta encoding, permite sincronizar archivos y directorios de manera incremental, minimizando el volumen de datos transferidos.
- **SSH:** Es un protocolo de red criptográfico que permite operar servicios de red de manera segura a través de una red no segura. El ejemplo más conocido de su aplicación es para entrada remota a sistemas informáticos por parte de los usuarios. Las aplicaciones más comunes incluyen inicio de sesión a través de línea de comandos a distancia y la ejecución remota de comandos, pero cualquier servicio de red se puede asegurar con SSH.

2.4.2.3. Herramientas de respaldo de información.

Entre las herramientas para el respaldo de la información, o los denominados backups tenemos almacenamiento en la nube y softwares o programas.

2.4.2.3.1. Bacula

Es un conjunto de programas de computadora que permite la realización de copias de seguridad en entornos informáticos, estos permiten crear una excelente gestión de las tareas realizadas. También se puede ejecutar por completo en un solo ordenador y hacer copias de seguridad de varios medios, incluyendo cintas y discos.

Este software se basa en una estructura cliente/servidor, que proporciona muchas características avanzadas en la gestión de almacenamiento de datos que hacen que sea más fácil encontrar y recuperar archivos perdidos o dañados. Debido a su estructura modular, este software es escalable desde sistemas informáticos pequeños y simples a sistemas que constan de cientos de ordenadores situados en una gran red.

Las principales características de la herramienta a destacar y que la consolidan como una herramienta de copia de seguridad sólida es:

- La estructura cliente/servidor, a través de su estructura modular independiente formada por el director, cliente, almacenamiento, bases de datos, la consola de administración.
- Posee licencia GPL, una licencia de derechos de autor ampliamente usada en el mundo del software libre y código abierto, en la cual se permite que los usuarios finales tengan libertad de usar, estudiar, compartir y modificar el software
- Varios canales de soporte por la comunidad, tales como, por ejemplo, listas de correo, foros, etc.
- Abundante documentación disponible en Internet.
- Portabilidad, la herramienta funciona en varios sistemas operativos.
- Característica que le permite ejecutar scripts o ejecutables antes y/o después del inicio de los trabajos.
- Manejo a través de la línea de comandos o interfaz gráfica de usuario.

Bacula está estructurado por los siguientes módulos, que operan de la siguiente manera:

- **Bacula Director:** Es el servidor de copia de seguridad en, responsable de la gestión de todos los procesos de copia de seguridad, restauración, verificación de datos y archivo de los mismos.
- **Bacula console:** Este programa permite que el administrador o el usuario pueda comunicarse con el Director, se puede ejecutar en cualquier ordenador de la red y en diferentes sistemas operativos.
- **Bacula File:** Este servicio, o cliente, es el software que está instalado en la máquina que va a ser protegida por la copia de seguridad, es decir, será responsable de enviar los archivos solicitados. Además es responsable de la gestión de restauración de archivos dirigido por el director.
- **Bacula Storage:** Es el software que gestiona la grabación y restauración de datos y sus atributos en los medios de copia de seguridad. Estos se pueden grabar directamente en volúmenes de datos en discos duros o dispositivos extraíbles.
- **Catálogo:** El servicio de catálogo es el programa responsable de mantener un índice de todos los archivos que se almacenan en la copia de seguridad y generar una base de datos de los volúmenes administrados por el Director. El catálogo agiliza la búsqueda de un archivo en la copia de seguridad en el momento en que el administrador del sistema tiene

que realizar una restauración, ya que mantiene una base de índice de los archivos grabados, la búsqueda de un archivo en el medio de volúmenes es más rápido.

2.4.2.3.2. Bacula Enterprise

Bacula Enterprise integra las características principales de los proyectos comunitarios Bacula, con tecnologías avanzadas específicas para crear una de las soluciones de backup y restauración de clase empresarial más potente y estable disponible. Incluye características exclusivas, así como plugins específicos para modernizar su estrategia de recuperación de datos, aumentar su eficiencia.

2.4.2.3.3. Amanda

AMANDA es un acrónimo de Advanced Maryland Automatic Network Disk Archiver, es un sistema automático de copia de seguridad en un solo servidor con soporte para múltiples medios de copia de seguridad, es similar a Bacula, se puede realizar copias de seguridad en varias estaciones de trabajo, tanto en el sistema operativo Windows, Linux, Unix, Mac OS, pero no tiene un sistema de gestión administrativa en la versión gratuita, convirtiéndose así en un software más técnico y manual.

Amanda utiliza formatos y utilidades nativas, por ejemplo, dump y GNU tar; y puede realizar copias de seguridad de un gran número de servidores y estaciones de trabajo que ejecutan varias versiones de Linux o Unix.

2.4.2.3.4. Amanda Enterprise

Amanda Enterprise contiene mejoras significativas en la facilidad de uso, seguridad, bases de datos y soporte de aplicaciones. Está disponible como una suscripción anual pagada que incluye actualizaciones en curso de funcionalidad y seguridad, así como apoyo técnico.

Las ventajas de la versión de pago de Amanda sobre la versión comunitaria se encuentran a continuación.

- Posibilidad de respaldo de bases de datos Oracle, SQL server, además servicios como Exchange y SharePoint.
- Copia de seguridad de máquinas virtualizadas basadas en VMware.
- Consola de administración basada en Web.

- Servicios profesionales y de soporte 24/7.
- Fácil instalación basada en asistente.
- Reportes de copia de seguridad.
- Administración basada en roles.
- La replicación del servidor de backup (en un sitio remoto).

2.4.2.3.5. BackupPC

Es un sistema de alto rendimiento de nivel empresarial para hacer copias de seguridad de equipos Unix, Linux, Windows, Mac OSX, ordenadores y portátiles en el disco de un servidor. BackupPC es altamente configurable y fácil de instalar y mantener. No se requiere el uso de clientes, ya que el servidor es en sí mismo es cliente para múltiples protocolos que son manejados por otros servicios nativos del sistema operativo.

Sus principales características son:

- Software de nivel empresarial que funciona con la arquitectura cliente/servidor.
- Software libre bajo la licencia GPL.
- Extrae los datos de la copia de seguridad a través herramientas nativas como: Samba, GNU tar, ssh, scp, rsync, rsyncd.
- Soporte de compresión opcional que reduce aún más el almacenamiento en disco.
- No se necesita la instalación de un cliente.
- Posee interfaz web para la gestión y administración.
- Fácil instalación y configuración.
- Posibilidad de ejecutar scripts pre y post copia de seguridad.
- Soporte de clientes Unix, Linux, Windows, Mac OSX.

2.4.2.3.6. Herramientas para amacenamiento en la nube

El almacenamiento en la nube se define como guardar archivos en un dispositivo remoto para acceso a la información almacenada, desde cualquier otro dispositivo, en cualquier lugar y por cualquier usuario que tenga autorización de acceso.

Entre las herramientas más comunes o utilizadas, tenemos:

- **DROPBOX:** Es el servicio de almacenamiento en la nube más utilizado. Ofrece de 2 GB hasta 16 GB de espacio gratuito. Dispone de aplicaciones para Windows, Mac, Linux, Android, BlackBerry e iOS y una aplicación oficial para teléfonos.
- **GOOGLE DRIVE:** Es una herramienta de Google, para su uso es necesario crear una cuenta de gmail. Permite almacenar y editar documentos. El almacenamiento básico y gratuito es de 15 GB, se puede adquirir más espacio contratando alguno de los planes disponibles. Google ha declarado que no accederá a los contenidos si no se lo exigen las autoridades, con lo que podemos decir que presta atención a la seguridad.
- **ONEDRIVE:** Este es un servicio de Windows, ofrece 7 GB gratis y la posibilidad de editar en línea, también cuenta con planes de pago. Respecto a la seguridad, Microsoft se reserva el derecho de analizar los archivos si el contenido le parece objetable.
- **MEGA:** Esta herramienta ofrece 50 GB gratuitos, al pagar un valor puede adquirir hasta 4 TB de almacenamiento y un servicio de encriptación de archivos. Es compatible con la mayoría de las plataformas y dispositivos, es de facil uso ya que tiene similitud con Google Drive o Dropbox. Además, incluye otras opciones de comunicación seguras.
- **MEDIAFIRE:** Es uno de los servicios de almacenamiento en la nube más antiguos de la lista. Obtendrás 50 GB si compartes enlaces y cumples ciertas premisas, pero puedes cargar archivos de hasta 25 MB, sin límite de ancho de banda. Cuenta demás con una aplicación móvil. Si en un año no entras, tu cuenta se eliminará, así que ten cuidado.

Respecto a la seguridad en la nube, actualmente existen varias opciones que permiten proteger los datos almacenados. Lo más relevante para la protección es el cifrado de datos. Existen diversas maneras de usar el cifrado, y puede ofrecerlas el proveedor de servicios en la nube o un proveedor de soluciones de seguridad en la nube:

- Cifrado de las comunicaciones con la nube en su totalidad.
- Cifrado de datos especialmente confidenciales, como las credenciales de las cuentas.
- Cifrado de extremo a extremo de todos los datos que se suben a la nube.

2.4.3. Confidencialidad de los Datos

Hay dos clases de encriptación utilizadas para brindar confidencialidad de los datos. Estas dos clases se diferencian en cómo utilizan las claves.

Los algoritmos de cifrado simétricos como (DES), 3DES y el Advanced Encryption Standard (AES) se basan en la premisa de que cada parte que se comunica conoce la clave precompartida. La confidencialidad de los datos también se puede garantizar utilizando algoritmos asimétricos, incluidos Rivest, Shamir y Adleman (RSA) y la infraestructura de clave pública (PKI, Public Key Infrastructure).

2.4.3.1. Cifrado Simétrico

Los algoritmos simétricos utilizan la misma clave precompartida para encriptar y desencriptar datos. Antes de que ocurra cualquier comunicación encriptada, el emisor y el receptor conocen la clave precompartida, también llamada clave secreta.

Tabla 16-2: Algoritmos de cifrado simétrico

Algoritmos de Cifrado Simétrico	Descripción
Data Encryption Standard (DES)	Este es un algoritmo de cifrado simétrico heredado. Puede utilizarse en modo de cifrado de flujo, aunque normalmente funciona en modo de bloque, cifrando los datos en un tamaño de bloque de 64 bits. El cifrado de flujo cifra un byte o un bit a la vez.
3DES (Triple DES)	Es una versión más reciente del DES, pero repite el proceso del algoritmo DES tres veces. El algoritmo básico ha sido bien probado en el campo durante más de 35 años. Se considera muy fiable cuando se implementa utilizando tiempos de vida clave muy cortos.
Advanced Encryption Standard (AES)	El AES es un algoritmo seguro y más eficiente que el 3DES. Es un algoritmo de cifrado simétrico popular y recomendado. Ofrece nueve combinaciones de longitud de clave y bloque usando una clave de longitud variable de 128, 192 o 256 bits para cifrar bloques de datos de 128, 192 o 256 bits de longitud.
Software-Optimized Encryption Algorithm (SEAL)	SEAL es un algoritmo de cifrado simétrico alternativo más rápido que el DES, 3DES y AES. Utiliza una clave de cifrado de 160 bits y tiene un menor impacto en la CPU en comparación con otros algoritmos basados en software.

Serie de Algoritmos Rivest ciphers (RC)	Este algoritmo fue desarrollado por Ron Rivest. Se han desarrollado varias variaciones, pero el RC4 es el más utilizado. RC4 es un cifrado de flujo y se usa para asegurar el tráfico web en SSL y TLS.

2.4.3.2. Cifrado Asimétrico

Los algoritmos asimétricos, también llamados algoritmos de claves públicas, están diseñados para que la clave de cifrado y la de descifrado sean diferentes. En cualquier plazo razonable, no es posible calcular la clave de descifrado a partir de la clave de cifrado, y viceversa.

Los algoritmos asimétricos utilizan una clave pública y una privada. Ambas claves son capaces de cifrar, pero se requiere la clave complementaria para el descifrado. El proceso también es reversible. Los datos cifrados con la clave privada requieren la clave pública para descifrarse. Los algoritmos asimétricos logran confidencialidad, autenticación e integridad mediante el uso de este proceso.

Entre algunos de los ejemplos de protocolos en los que se utilizan algoritmos de claves asimétricos se incluyen los siguientes:

- **Intercambio de claves por Internet (IKE, Internet Key Exchange)-** Esto es un componente fundamental de las IPsec VPNs.
- **Secure Socket Layer (SSL) –** Esto se implementa ahora como el estándar de Seguridad de la Capa de Transporte (TLS) de la IETF.
- **Secure Shell (SSH) –** Este protocolo proporciona una conexión segura de acceso remoto a dispositivos de red.
- **Pretty Good Privacy (PGP) –** Este programa de computadora proporciona privacidad y autenticación criptográfica. A menudo, se utiliza para aumentar la seguridad de las comunicaciones por correo electrónico.

Los algoritmos asimétricos son sustancialmente más lentos que los simétricos. Su diseño se basa en problemas informáticos, como la factorización de números demasiado grandes o el cálculo de logaritmos discretos de números demasiado grandes. Dado que carecen de velocidad, los algoritmos asimétricos se utilizan típicamente en criptografías de poco volumen, como las firmas digitales y el intercambio de claves.

A continuación se describen ejemplos comunes de algoritmos de cifrado asimétrico.

Tabla *17*-2: *Algoritmos de cifrado asimétrico*

Algoritmo de Cifrado Asimétrico	Descripción
Diffie-Hellman (DH)	El algoritmo Diffie-Hellman permite a dos partes acordar una clave que pueden utilizar para cifrar los mensajes que quieren deseean mutuamente. La seguridad de este algoritmo depende de la suposición de que es fácil elevar un número a una cierta potencia, pero difícil calcular qué potencia se utilizó dado el número y el resultado.
Digital Signature Standard (DSS) y Digital Signature Algorithm (DSA)	El DSS especifica el DSA como el algoritmo para las firmas digitales. DSA es un algoritmo de clave pública basado en el esquema de firma de ElGamal. La velocidad de creación de la firma es similar a la del RSA, pero es de 10 a 40 veces más lenta para la verificación.
Rivest, Shamir, and Adleman encryption algorithms (RSA)	RSA es para la criptografía de clave pública que se basa en la dificultad actual de factorizar números muy grandes. Es el primer algoritmo que se conoce que es adecuado para la firma así como para el cifrado. Se utiliza ampliamente en los protocolos de comercio electrónico y se cree que es seguro si se le dan claves suficientemente largas y el uso de implementaciones actualizadas.
EIGamal	Un algoritmo de cifrado de clave asimétrica para la criptografía de clave pública que se basa en el acuerdo de clave Diffie-Hellman. Una desventaja del sistema de ElGamal es que el mensaje cifrado se vuelve muy grande, aproximadamente dos veces el tamaño del mensaje original y por esta razón sólo se utiliza para mensajes pequeños como claves secretas.

CAPÍTULO III

3. METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Tipo y Diseño del Estudio

3.1.1. Tipo de la Investigación

Esta tesis se compone de una investigación descriptiva y aplicada, se fundamenta en conocimientos existentes, por procedimientos metodológicos de estudios previos utilizados en la preservación digital de documentos que ayuden a formular pautas de preservación a largo plazo. La investigación también es tipo experimental ya que se verifica si la hipótesis planteada tiene validez en el marco de trabajo.

3.1.2. Diseño de la Investigación

La investigación es del tipo cuasi-experimental ya que se analiza modelos existentes, leyes, normativas, políticas de buenas prácticas que servirán de apoyo para la implementación del modelo de Preservación Digital de Documentos a Largo Plazo, de manera particular en sus diferentes etapas de realización se integran técnicas de investigación como la revisión bibliográfica, la observación comparativa, el cuestionario, el test y la entrevista.

3.2. Método de la Investigación

Se utiliza el método científico, mediante el mismo en las diferentes fases se revisará información en libros, revistas, artículos científicos e Internet, lo que permite detectar los problemas actuales de preservación digital de documentos a largo plazo y obtener un conocimiento válido desde el punto de vista científico, utilizando herramientas fiables, el procedimiento a seguir es:

- Planteamiento del problema
- Formulación dela hipótesis
- Levantamiento de la información (Registros, Internet, bibliografía científica, investigaciones realizadas a nivel nacional e internacional)
- Implementación del modelo de Preservación de Documentos a Largo Plazo.
- Análisis e interpretación de resultados

- Comprobación de la hipótesis

Método deductivo una vez analizado los problemas que existen en la Preservación Digital de Documentos se trata de encontrar un modelo de que cumpla con las falencias existentes en la preservación basado en OAIS, PREDECI, DAMM, PREMIS y evaluado por Néstor.

3.3. Enfoque de la Investigación

La investigación presenta un enfoque cuantitativo debido a que responde preguntas de investigación sobre Preservación Digital de Documentos y sus retos actuales, que ayudara a establecer un modelo de preservación a Largo Plazo.

3.4. Alcance de la Investigación

La finalidad del análisis de los modelos de preservación digital de documentos es cubrir la necesidad desde la perspectiva funcional, de organización y niveles de estado de prácticas de preservación digital para apoyar la definición de un modelo con elementos funcionales, conceptuales y de buenas prácticas que sirvan de argumentos clave para integrar una propuesta de estrategia de preservación a largo plazo. Cabe reiterar que este análisis pretende definir a nivel conceptual, funcional y de buenas prácticas refiriendo por ello a abstracciones de las figuras clave de conceptos y funciones técnicas generales de los sistemas de preservación digital documentos. El alcance de análisis técnico se limitará a un nivel elemental (no a nivel técnico avanzado de programación y códigos) ya que el interés primordial es que los resultados sirvan de modo pragmático y conceptual para entender los niveles funcionales y operativos de los sistemas de preservación digital documental en sus posibilidades y requerimientos de seguridad de la información y necesidades de buenas prácticas.

3.5. Población

La población de la investigación está formada por todas aquellas personas utilizan documentos informáticos.

3.6. Selección de la Muestra

Para el estudio se considera que el universo será la misma cantidad de la población y la muestra será igual al universo.

3.7. Tamaño de la Muestra

La muestra para la investigación será igual a la población.

Se establece el tamaño de la muestra en función de la Fórmula (Willan GOO, De, Raúl Hatt).

$$n = \frac{N\sigma^2 Z^2}{e^2(N-1) + \sigma^2 Z^2}$$

Donde:

n = el tamaño de la muestra.

N = tamaño de la población ().

$\sigma =$ Desviación estándar de la población equivalente a un valor constante de 0,5.

Z = Valor obtenido mediante niveles de confianza. Nivel de confianza deseado (1,645) valor para el 90%

e = Límite aceptable de error maestral (0,1) para el 10 %.

$$n = \frac{20 \cdot 0{,}5^2 \cdot 1{,}645^2}{0{,}1^2(20-1) + 0{,}5^2 \cdot 1{,}645^2}$$

$$n = \frac{13{,}5301}{0{,}8665} = 15{,}41$$

Estableciéndose el tamaño de la muestra en 15 personas que deben ser consideradas para el estudio, para lo cual serán seleccionadas en función al número de personas que trabajen en las áreas categorizadas en la población.

3.8. Técnicas de Recolección de datos Primarios y Secundarios

Se basa en revisión de fuentes de información bibliográficas primarias como Pruebas y Observación de resultados y secundarias como:

- Leyes ecuatorianas e internacionales referentes a la Preservación Digital de Documentos.
- Artículos científicos en base de datos de bibliotecas virtuales
- Tesis realizadas nacionales e internacionales de cuarto nivel
- Trabajos de investigaciones nacionales e internacionales
- Conferencias académicas, congresos, seminarios
- Revistas indexadas y no indexadas publicadas de prestigio
- Páginas de internet que brinden información confiable.

3.9. Instrumentos de Recolección de datos Primarios y Secundarios

La recolección de datos utilizada será la Néstor con el cumplimiento de un checklist antes y después de la implementación de un Modelo de Preservación Digital de Documentos a Largo Plazo para buscar información que será útil para evaluar los indicadores de las variables.

3.10. Instrumentos para Procesar los datos Recopilados

Como instrumentos para procesar los datos recolectados se utiliza el software Microsoft Excel para la tabulación y análisis estadístico de las encuestas aplicadas.

3.11. Directrices de la Preservación Digital

Según la UNESCO las directrices poseen 41 principios teóricos que hablan sobre la doctrina de la preservación digital y que a su vez se agrupan en 11 materias fundamentales.

Directrices:

1. Patrimonio
2. Preservación Digital
3. Responsabilidad
4. Decidir que Conservar
5. Colaborar con los Productores
6. Derechos
7. Control
8. Autenticidad y Protección de Datos

9. Mantenimiento de la Accesibilidad
10. Gestión
11. Trabajo en Equipo

Estas directrices sirven como guía para personas o instituciones que tengan responsabilidad con la preservación digital. Las mismas que establecen el tipo de público (usuarios) al que va dirigido y el tipo de información que pueden acceder.

- Planificadores: son los principios básicos de la preservación digital que sirven para establecer las políticas.
- Altos Directivos: son las bases conceptuales de la preservación digital, así como los problemas de gestión que se genera en los programas de preservación.
- Directores de Servicio: son los que toman las decisiones sobre la información conceptual y de gestión.
- Especialistas técnicos: son los que conocen toso sobre los aspectos técnicos de los programas de preservación.

3.11.1. Directrices de la Preservación Digital

Tabla 1-3: Directrices de Preservación Digital según (UNESCO, 2003)

Directrices	***Definición***
Patrimonio	No todos los objetos digitales merecen ser conservados. El patrimonio digital está constituido únicamente por los objetos que poseen valor permanente. La continuidad de la existencia de los objetos dignos de ser conservados es un factor decisivo, si se pierda el acceso a grandes volúmenes de datos la posibilidad de recuperarlos en ínfima. La continuidad requiere de una acción sostenida y directa denominada preservación digital.
Preservación Digital	La preservación consiste en mantener la capacidad de presentar los elementos esenciales de os objetos digitales auténticos. La preservación digital puede hacer frente a los peligros, amenazas que sufren los objetos digitales (material, lógico, conceptual y esencial).
Responsabilidad	Las entidades y personas deben asumir responsabilidades para lograr la preservación digital. No todos tienen que hacer toso, y no todo tiene que hacerse de inmediato. Deberían existir programas de preservación completos y solventes. Se debe avanza en pequeños pasos a que no avanzar nada.

	Los responsables deben tener en cuenta que existen problemas complejos; y lo importante es no provocar daños, y que los procesos se desarrollen en su totalidad. Se debe decir de manera clara, explicita y seria las responsabilidades.
Decir que Conservar	Las decisiones de selección deben ser fundamentadas, coherentes y responsables. La decisión de conservar un elemento puede ser revisado después, pero cuando se decide no presérvalo la decisión es definitiva.
Colaborar con los Productores	La preservación debe hacer frente a las tendencias de las tecnologías digitales y a sus modalidades de desarrollo y utilización. Los objetos digitales se crean sin intención de preservarlos a largo plazo. Se debe colaborar con los productores en el desarrollo de las normas y prácticas.
Derechos	La preservación debe tener derecho legal a reunir, copiar, denominar, modificar, preservar y proporcionar acceso a los objetos digitales.
Control	Se los debe transferir a un lugar seguro donde puedan ser preservados, controlados, protegidos y gestionados los elementos de patrimonio. Los objetos pueden ser identificados y descritos mediante metadatos que son conservados, gestionados y descubiertos por los recursos. Se debe hacer una documentación apropiada para acciones futuras como las características de los productos digitales. Los programas de preservación deben utilizar sistemas de metadatos que facilitan la interoperabilidad entre programas. Se debe proteger de manera eficaz los vínculos entre objetos digitales y sus metadatos.
Autenticidad y protección de Datos	La autenticidad característica fundamental cuando los objetos digitales son utilizados como pruebas. Se debe garantizar la seguridad en el almacenamiento y gestión de datos. Los programas de preservación deben hacer frente a problemas de autenticidad con procedimientos que son modificados cuando se crea necesario. La autenticidad son medidas que garantiza la integridad de los datos y documentos. La redundancia de los sistemas y la seguridad brindan protección a los datos, aquí se debe incluir copias de seguridad que deben ser almacenadas de manera segura porque conservar datos a largo plazo.
Mantenimiento de la Accesibilidad	Para mantener la accesibilidad se deben hacer métodos económicos que garantizan el acceso cada vez que sea necesario. Los programas deben encontrar métodos para preservar el acceso a objetos poco normalizados, en un entorno en el que las normas evolucionan rápidamente. El acceso a los datos digitales siempre depende de una combinación de equipos y programas informáticos. Los programas optan por estrategias múltiples para preservar el acceso a los datos. Se deberán tener en cuenta los beneficios potenciales del hecho de conservar los flujos de datos originales de los objetos, así como las versiones modificadas, como un seguro contra cualquier fallo de estrategias aún inciertas. Las estrategias para preservar la accesibilidad no son autónomas, sino que son respaldadas por otras responsabilidades. Además, pueden combinarse varias estrategias para obtener mejores resultados.

	Los programas de preservación deben decidir qué niveles de pérdidas son aceptables o no, tanto en lo relativo a elementos y objetos como a necesidades de los usuarios.
Gestión	Se debe tener conocimiento sobre los diversos aspectos de preservación digital para tomar las decisiones correctas en el momento adecuado. La preservación integra le evaluación y la gestión de riegos. Se debe fijar prioridades por la cantidad de material que se maneja. Los programas de preservación son difíciles de evaluar porque engloban muchas incertidumbres, como la constante evolución de las técnicas y tecnologías y los plazos de conservación prolongados. Los programas de preservación pueden empezar como proyectos piloto, aunque, con el tiempo, se requerirán modelos de gestión duraderos. Se puede recurrir a proveedores de servicios para algunas tareas, el cumplimiento de los objetivos de preservación es responsabilidad de los programas de preservación y de quienes los supervisan.
Trabajo en Equipo	Se realiza colaboración para elaborar programas de preservación porque aportan una amplia cobertura. Los beneficios potenciales de dan por la colaboración entre costos y decisiones.

Realizado por: Marilú Torres, 2021

3.11.2. Comparación de las Directrices de Unesco con los Modelos de Preservación Digital

Tabla 2-3: Comparación de los Modelos de Preservación con las Directrices

	MODELOS DE PRESERVACIÓN DIGITAL			
Directrices	***PREDECI***	***OAIS***	***PREMIS***	***DAMM***
Patrimonio	1	1	1	1
Preservación Digital	3 (Preservation Planning)	2(Área de Almacenamiento)	3(Entidad Intelectual)	3(DAMM)
Responsabilidad	3 (Preservation Planning)	3(Administration)	2(Usa Matadatos de preservación)	3(Level 1)
Decidir que conservar	3 (Ingest)	2(Ingesta)	3(Entidad Objeto)	3(Level 6)
Colaborar con los Productores	1	1	1	1
Derechos	1	3(Administration)	3(Derechos)	1
Control	3 (Administration)	2(Administration)	1	2(Level 2)
Autenticidad y Protección de los Datos	3 (Archival Storage)	3(Plan de Preservación)	3(Acontecimientos)	3(Level 3)

Mantenimiento de la Accesibilidad	3 (Data Management) 3 (Acceso)	2(Acceso)	3(Agentes)	3(Level 4) 3(Level 5)
Gestión	3 (Data Management)	2(Data Management)	1	1
Trabajo en Equipo	1	1	1	1

Realizado por: Marilú Torres, 2021

Valoración

- 1. No cumple
- 2. Cumple Parcialmente
- 3. Cumple Totalmente

Después de hacer la comparación entre las directrices con los modelos de Preservación se observar que los ítems cumplen con la valoración dada por las directrices.

Tabla 3-3: Análisis de los Modelos de Preservación en base a las directrices de la UNESCO

	MODELOS DE PRESERVACIÓN DIGITAL			
Directrices	***PREDECI***	***OAIS***	***PREMIS***	***DAMM***
Patrimonio	1	1	1	1
Preservación Digital	3	2	3	3
Responsabilidad	3	3	2	3
Decidir que conservar	3	2	3	3
Colaborar con los Productores	1	1	1	1
Derechos	1	3	3	1
Control	3	2	1	2
Autenticidad y Protección de los Datos	3	2	3	2
Mantenimiento de la Accesibilidad	3	2	3	3
	3			3
Gestión	2	1	1	1
Trabajo en Equipo	1	1	1	1
PROMEDIO	2,25	1,66	1,83	2

Realizado por: Marilú Torres, 2021

Tabla 4-3: Porcentaje de Cumplimiento de los Modelos con las directrices

Modelo	*Porcentaje*
PREDECI	75%
OAIS	55,33%
PREMIS	61%
DAMM	66,66%

Realizado por: Marilú Torres, 2021

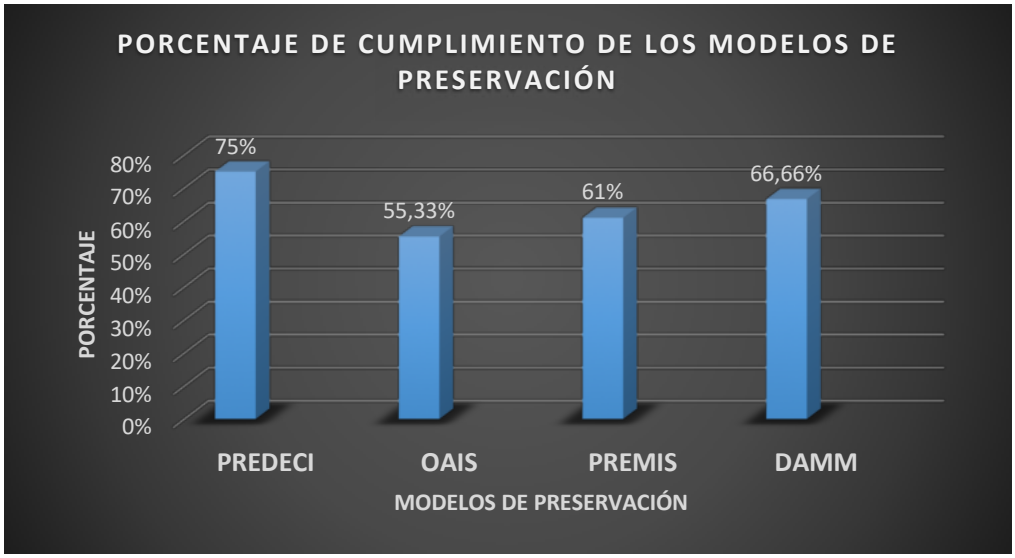


Gráfico 1-3: Análisis de los Modelos de Preservación en base a las directrices de la UNESCO
Realizado por: Marilú Torres, 2021

El modelo de preservación que cumple las directrices de la Unesco es PREDECI con un porcentaje de 75 % de cumplimiento, lo cual servirá como base en el proyecto de investigación.

3.11.3. Comparación entre la Norma ISO/IEC 27001 y los Modelos de Preservación Digital

Análisis Comparativo de los Modelos de Preservación Digital con la Norma ISO/IEC 27001

Tabla 5-3: Cuadro Comparativo

	PREDECI	***OAIS***	***PREMIS***	***DAMM***
Integridad	3	3	2	1
Disponibilidad	3	2	2	3
Confidencialidad	2	1	3	1
Total	2,666	2	2,333	1,666

Realizado por: Marilú Torres, 2021

Valoración

- 1. No Cumple
- 2. Cumple Parcialmente
- 3. Cumple Totalmente

Tabla 6-3: Porcentaje del análisis de los Modelos de preservación con las Norma ISO 27001

Modelo	***Porcentaje***
PREDECI	88,66%
OAIS	66,66%
PREMIS	77,66%
DAMM	55,33%

Realizado por: Marilú Torres, 2021

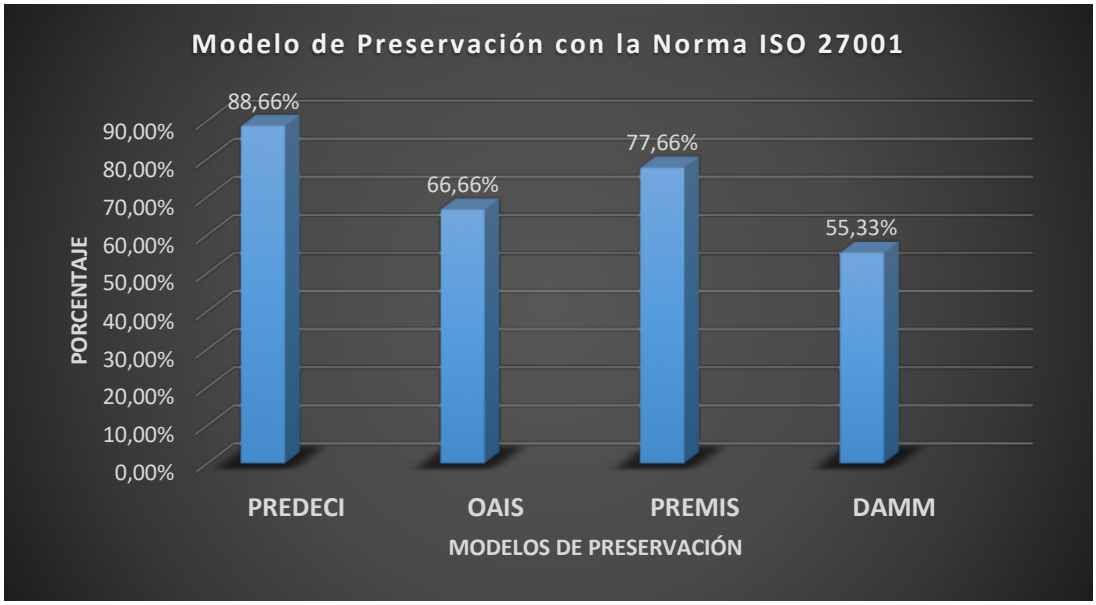


Gráfico 2-3:Análisis de los Modelos de Preservación con las Normas ISO/IEC 27001
Realizado por: Marilú Torres, 2021

El modelo que más cumple los criterios de la Norma ISO/IEC 27001 es el modelo PREDECI con un porcentaje de 88,66% de cumplimiento, lo cual será aplicado en el proyecto de investigación.

3.11.4. Comparación entre los Criterios de NESTOR y los Modelos de Preservación Digital

Tabla 7-3: Análisis de cumplimiento de Criterios NESTOR con los Modelos de Preservación Digital

Requisitos Básicos NESTOR	*MODELOS DE PRESERVACIÓN DIGITAL*			
	PREDECI	**OAIS**	**PREMIS**	**DAMM**
Responsabilidad con los documentos Digitales	2	2	2	2
Organización	2	2	2	1
Legalidad	2	2	2	1
Eficiencia y Eficacia en las Políticas	2	1	2	1
Infraestructura Técnica adecuada	2	1	1	2
Adquisición	2	2	1	2
Integridad, autenticidad y usabilidad en la conservación del objeto digital	2	2	2	2

Gestión de Metadatos y existencia de auditoria	2	2	1	1
Difusión	2	2	2	1
Planificación	2	2	2	2
Total	20	18	17	15

Realizado por: Marilú Torres, 2021

Valoración:

- 1. No cumple
- 2. Si Cumple

Tabla 8-3: Porcentaje del análisis de los modelos de preservación con Criterios NESTOR

Modelo	***Porcentaje***
PREDECI	100%
OAIS	90%
PREMIS	85%
DAMM	75%

Realizado por: Marilú Torres, 2021

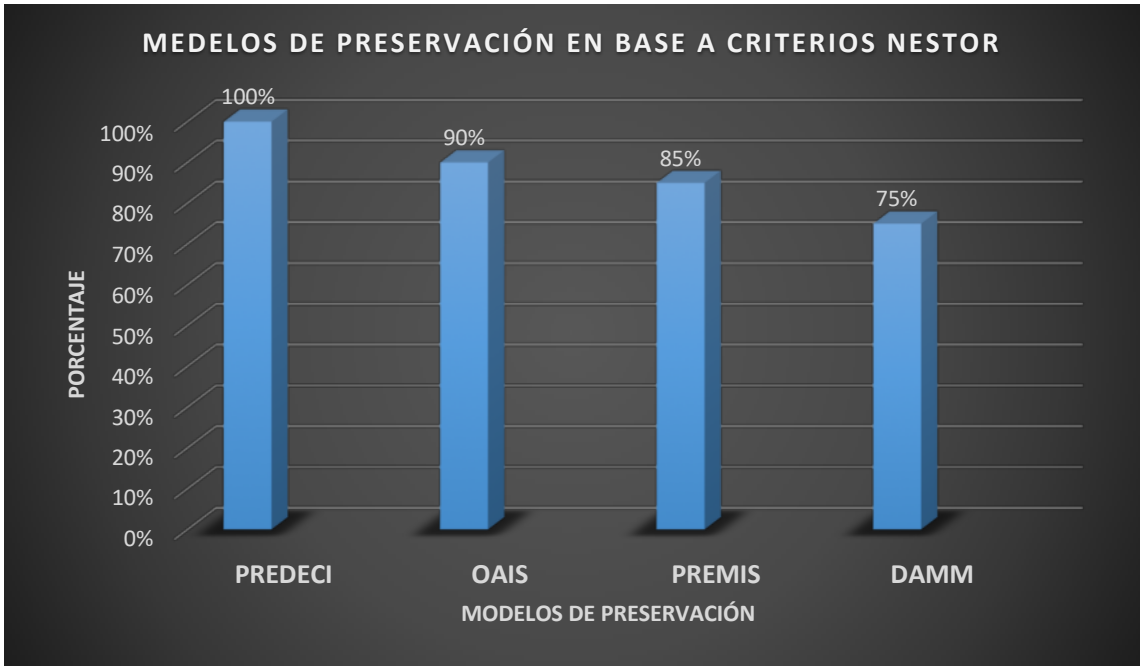


Gráfico 3-3: Porcentaje del análisis de los Modelos de preservación con criterios NESTOR
Realizado por: Marilú Torres, 2021

El modelo de preservación que cumple los criterios de NESTOR es PREDECI con un porcentaje de 100% de cumplimiento, lo cual servirá como base en el proyecto de investigación.

Una vez realizado los análisis de los modelos de Preservación Digital en base a diferentes aspectos, Directrices de la Unesco, Normas ISO/IEC 27001 y criterios de NESTOR, se ha seleccionado el modelo que posee mayor cumplimiento, en la siguiente tabla se puede observar los porcentajes en general.

Tabla 9-3: Porcentaje de Cumplimiento de Modelos

	Modelos de Preservación Digital			
	PREDECI	**OAIS**	**PREMIS**	**DAMM**
Directrices Unesco	75%	55,33%	61%	66,66%
Norma ISO/IEC 27001	88,66%	66,66%	77,66%	55,33%
Criterios de NESTOR	100%	90%	85%	75%
Total	87,88%	70,66%	74,55%	65,66%

Realizado por: Marilú Torres, 2021

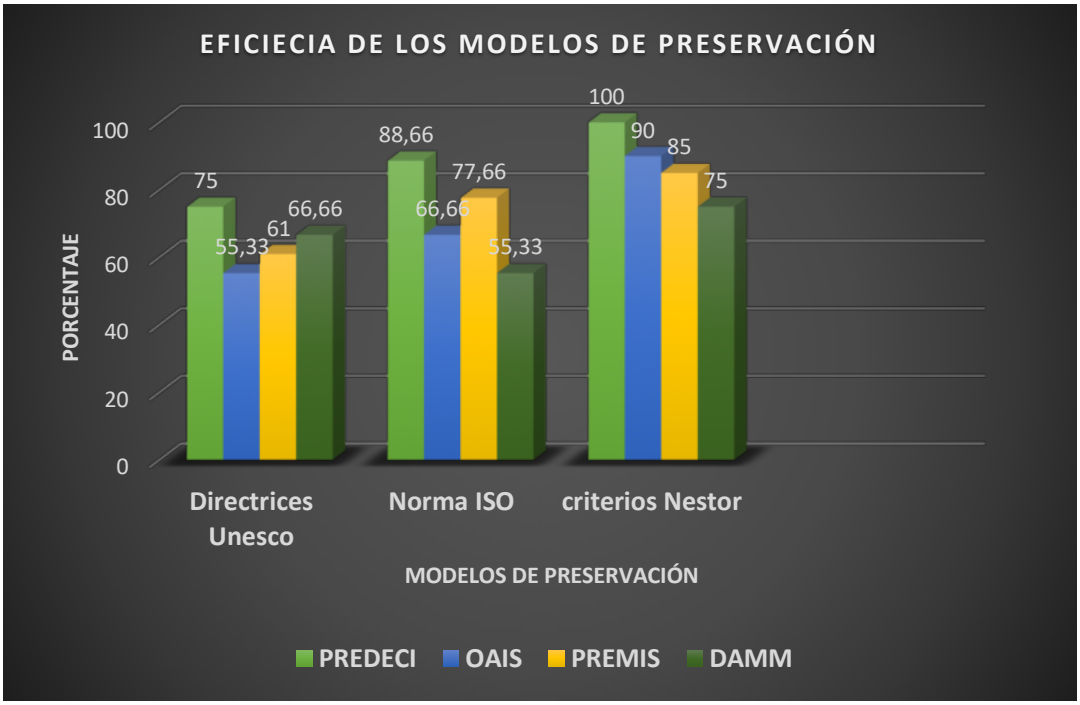


Gráfico 4-3: Eficiencia de los Modelos de Preservación
Realizado por: Marilú Torres, 2021

Porcentaje Final de Cumplimiento y Efectividad

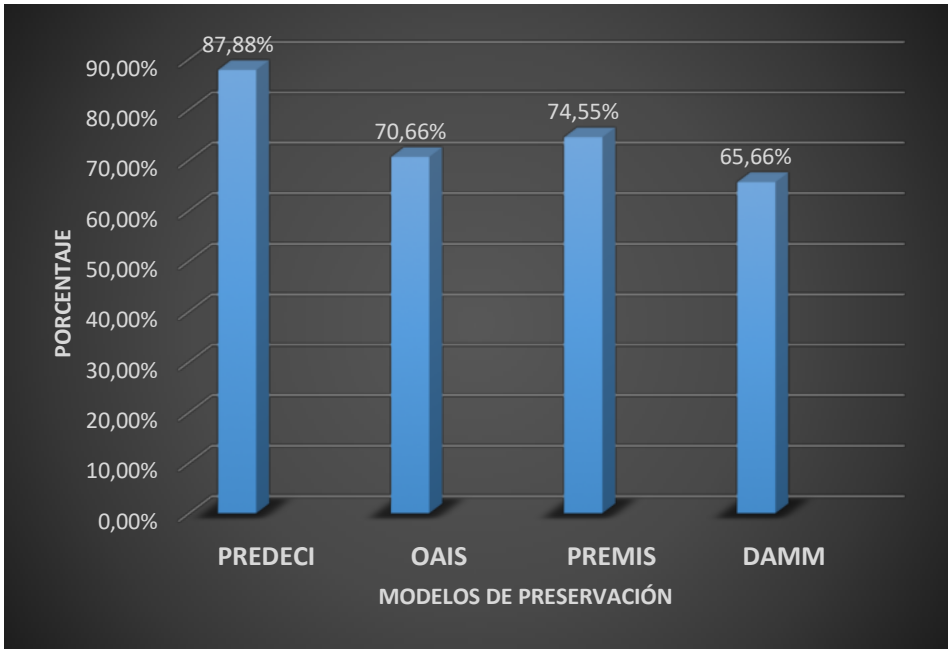


Gráfico 5-3: Porcentaje Final de Cumplimiento y Efectividad
Realizado por: Marilú Torres, 2021

Se realizó el análisis comparativo de los modelos de preservación digital OAIS, PREDICE, PREMIS y DAMM; donde se evaluó distintas características como directrices de la Unesco, Norma ISO/IEC 27001 y Criterios NESTOR, que permitió seleccionar el modelo más óptimo. El modelo seleccionado cumple con todas características y el modelo de preservación Digital PREDECI tiene un porcentaje mayor de cumplimiento de 87,88 % como se muestra en la figura 23.

CAPÍTULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Análisis de la situación actual

Dentro de la encuesta realizada se establece la probabilidad de ocurrencia establecido en función del promedio de las respuestas obtenidas a las preguntas establecidas para la evaluación de cada ítem; es así que el cálculo de la probabilidad de ocurrencia del riesgo evaluado es igual a:

$$Probabilidad = \frac{Promedio\ de\ Respuestas\ negativas}{Total\ de\ la\ población\ encuestada}$$

Primera encuesta del antes de cómo era la aplicación y la existencia de la preservación digital a largo plazo. El resultado de las encuestas del antes de aplicar el modelo de preservación digital se obtuvo los siguientes datos para cada uno de las preguntas.

1.- ¿Conoce usted si existen controles, normas para Archivar de manera correcta la Información en las instituciones?

SI ( )

NO ( )

Tabla 1-4: Porcentaje de la Pregunta 1

NO	SI
11	4
73,33%	26,67%

Realizado por: Marilú Torres, 2021

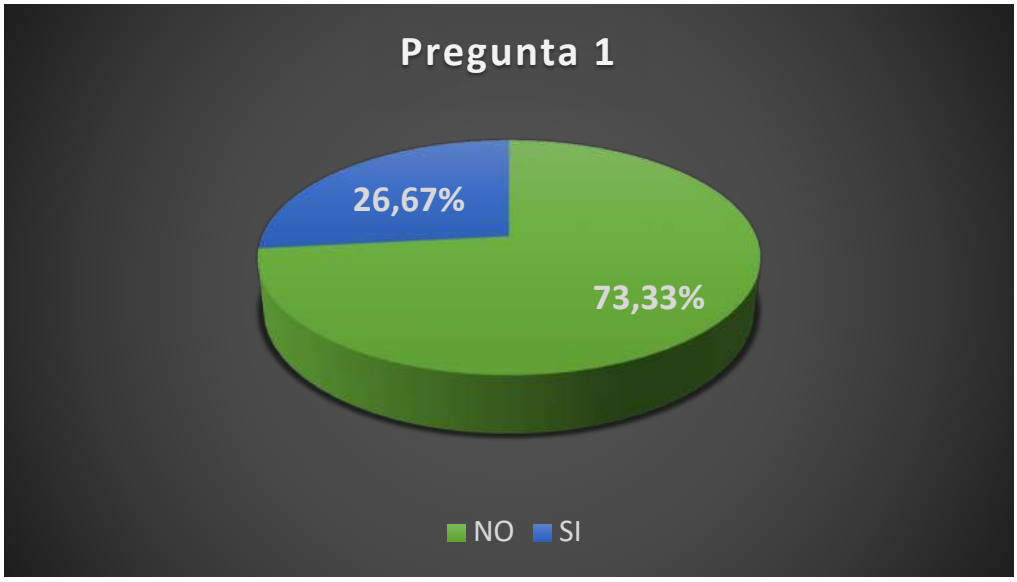


Gráfico 1-4: Porcentaje de la Segunda Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 73,33% de las personas encuestadas respondió que no existen controles para archivar la información dentro de las instituciones, mientras que el 26,67% manifestaron que si existen controles para archivar la información.

2.- ¿Conoce Usted sobre la Preservación Digital a Largo Plazo?

SI ( )
NO ( )

Tabla 2-4: Porcentaje de la Pregunta 2

NO	SI
9	6
60%	40%

Realizado por: Marilú Torres, 2021

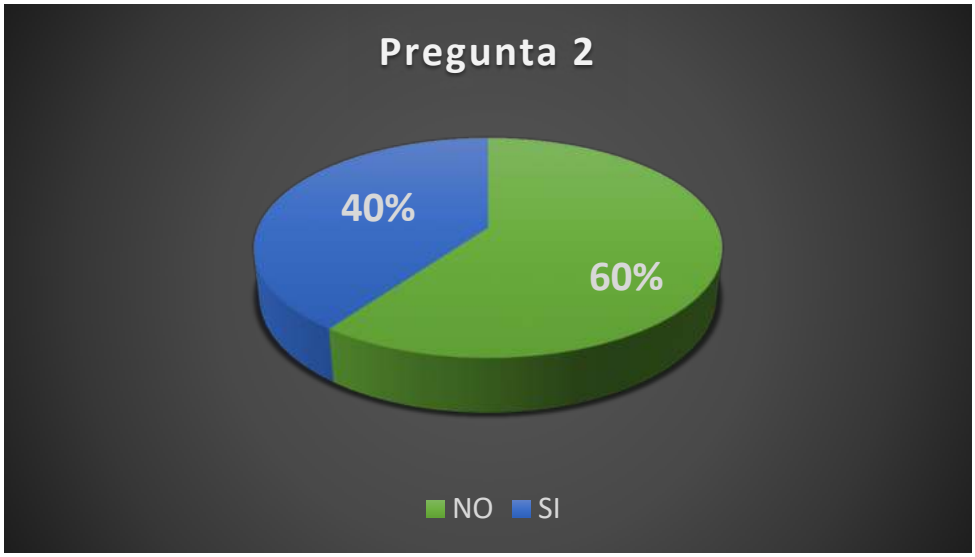


Gráfico 2-4: Porcentaje de la Segunda Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 60% de las personas encuestadas respondió que no sabe sobre el tema de preservación digital a largo dentro de las instituciones, mientras que el 26,67% manifestaron que si conocen sobre el tema de preservación digital dentro de las instituciones.

3.- ¿Sabe usted si la información es recopilada o preservada en las instituciones?

SI ( )
NO ( )

Tabla 3-4: Porcentaje de la Pregunta 3

NO	SI
12	3
80%	20%

Realizado por: Marilú Torres, 2021

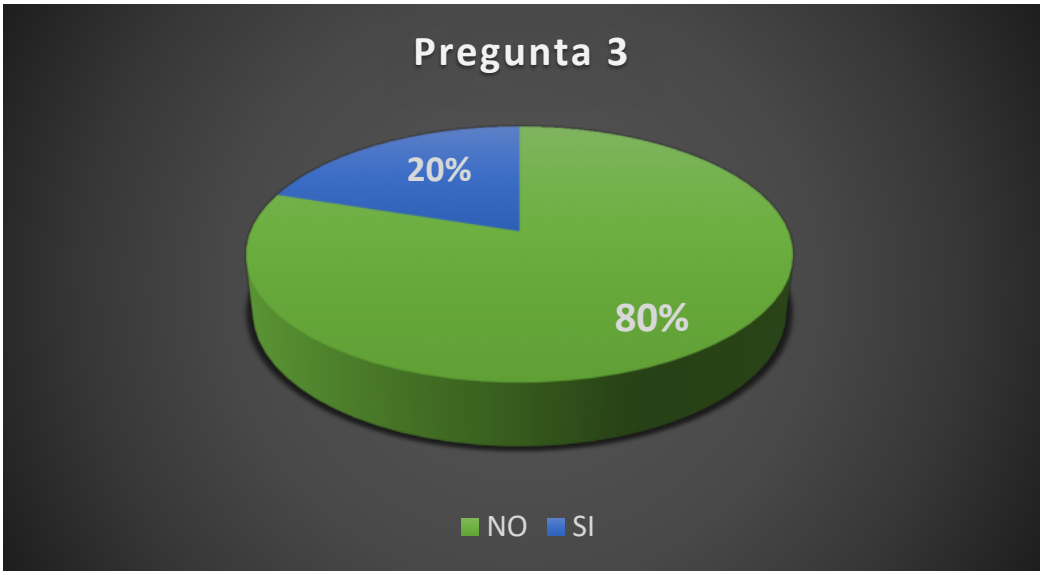


Gráfico 3-4: Porcentaje de la Tercera Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 80% de las personas encuestadas respondió que desconoce que las instituciones recopilen o preserven información, mientras que el 26,67% manifestaron que si saben que algunas instituciones recopilan o preservan información.

4.- ¿Sabe usted si se aplica preservación digital a la información en la actualidad?

SI ( )
NO ( )

Tabla 4-4: Porcentaje de la Pregunta 4

NO	SI
8	7
53,33%	46,67%

Realizado por: Marilú Torres, 2021

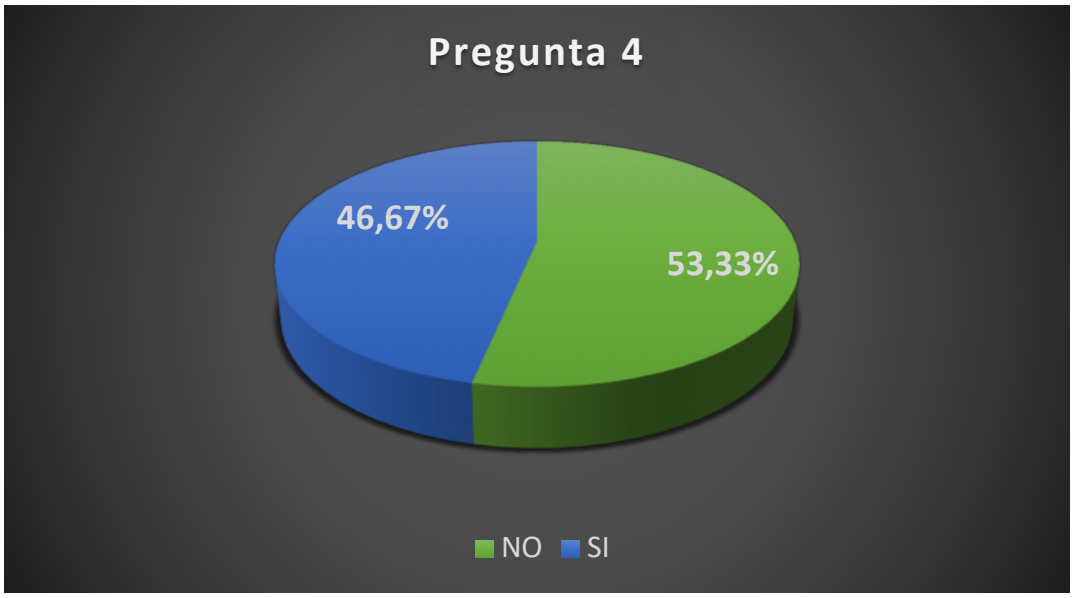


Gráfico 4-4: Porcentaje de la Cuarta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 53,33% de las personas encuestadas respondió que desconoce que se aplique preservación digital a la información en la actualidad dada por las instituciones, mientras que el 26,67% manifestaron que si saben que se aplica preservación digital a la información en la actualidad dentro de las diferentes instituciones.

5.- ¿Cómo es la eficiencia en la atención del usuario (cliente) para obtener información?

Mala ( )

Buena ( )

Excelente ( )

Tabla 5-4: Porcentaje de la Pregunta 5

Mala	Buena	Excelente
5	6	4
33,33%	40%	26,67%

Realizado por: Marilú Torres, 2021

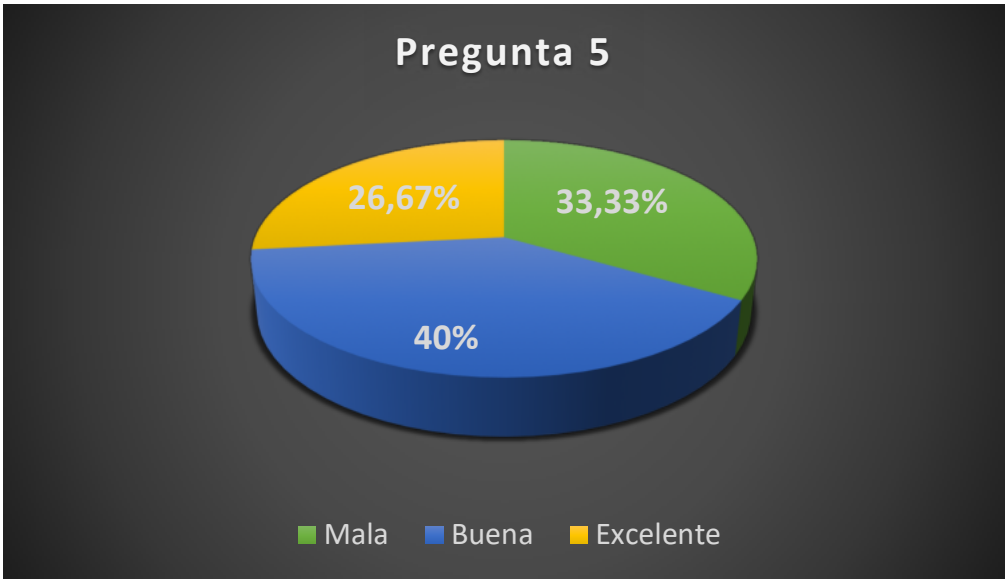


Gráfico 5-4: Porcentaje de la Quinta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 40 % de las personas encuestadas respondió que la atención a los usuarios (Clientes) es mala dentro de las diferentes instituciones, mientras que el 33,33% respondió que es buena y el 26,67% manifestaron que la atención a los usuarios (clientes) dentro de las diferentes instituciones es excelente.

6.- ¿Cree usted que la producción de Preservación Digital permite gestionar la información de manera adecuada dentro de las instituciones?

SI ( )
NO ( )

Tabla 6-4: Porcentaje de la Pregunta 6

NO	SI
9	6
60%	40%

Realizado por: Marilú Torres, 2021

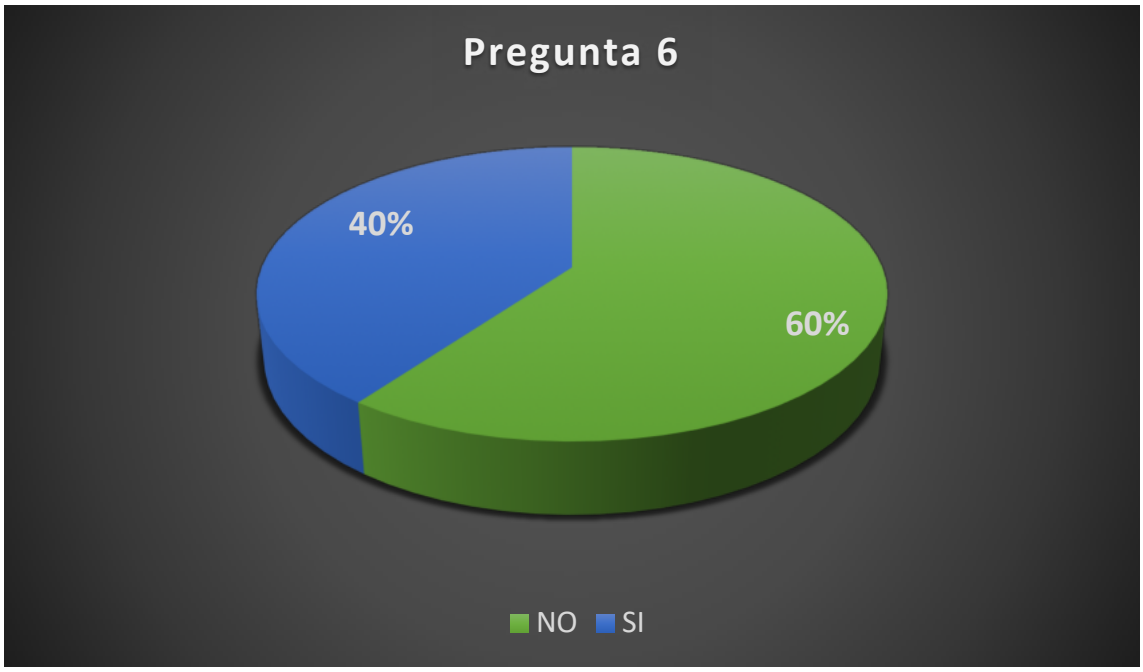


Gráfico 6-4: Porcentaje de la Sexta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 60 % de las personas encuestadas respondió que la producción de preservación digital no permite gestionar de manera eficiente la información dentro de las instituciones mientras que el 40 % respondió que la producción de preservación digital permite gestionar de manera eficiente la información de las diferentes instituciones es buena.

7.- ¿Cree usted que las personas manejan la tecnología de manera correcta en la preservación digital dentro de las instituciones?

SI ( )
NO ( )

Tabla 7-4: Porcentaje de la Pregunta 7

NO	SI
11	4
73,33%	26,67%

Realizado por: Marilú Torres, 2021

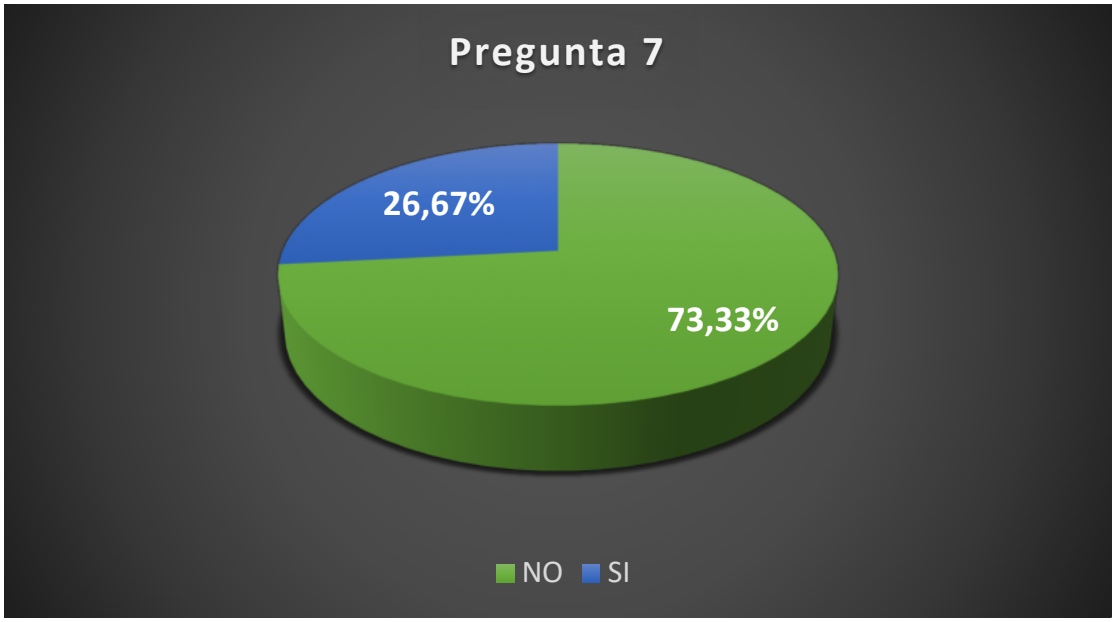


Gráfico 7-4: Porcentaje de la Séptima Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 73,33 % de las personas encuestadas respondió que no existen personas que manejen la tecnología de una manera correcta en la preservación digital dentro de las diferentes instituciones, mientras que el 26,67 % respondió que si existen personas que manejen la tecnología de una manera correcta en la preservación digital dentro de las diferentes instituciones.

8.- ¿Cree usted que las medidas de Seguridad para evitar la pérdida de la información en Preservación Digital son:

Mala ( )

Buena ( )

Excelente ( )

Tabla 8-4: Porcentaje de la Pregunta 8

Mala	Buena	Excelente
8	4	3
53,33%	26,67%	20%

Realizado por: Marilú Torres, 2021

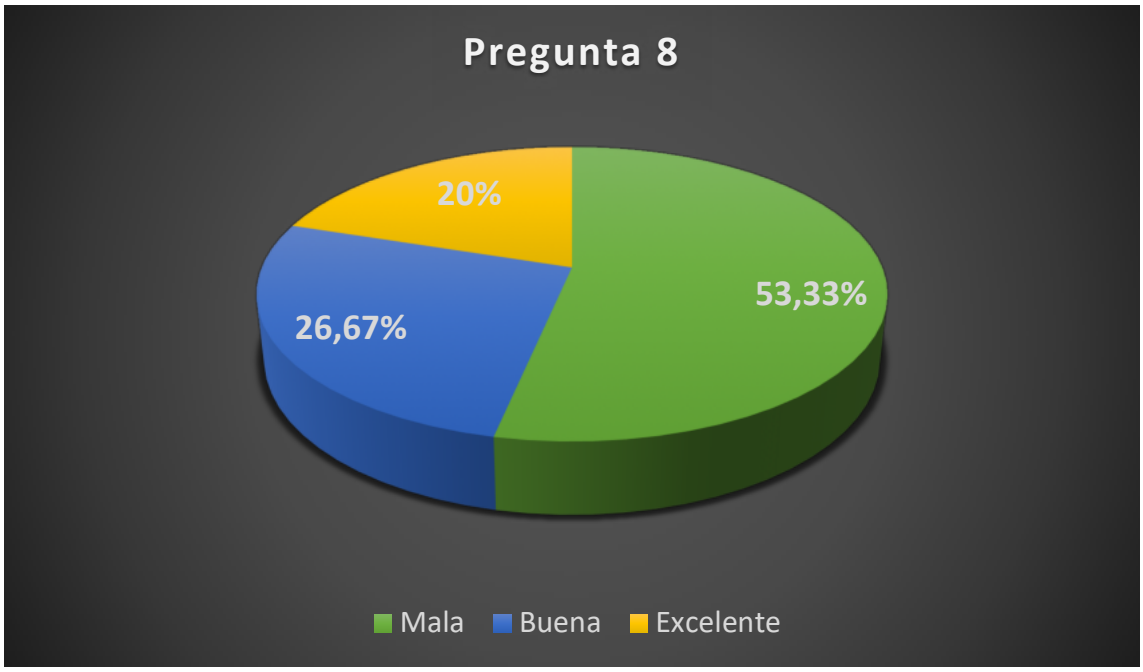


Gráfico 8-4:Porcentaje de la Octava Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 53,33 % de las personas encuestadas respondió que las medidas de Seguridad para evitar la pérdida de la información en Preservación Digital no existen dentro de las diferentes instituciones mientras que el 26,67% respondió que son buenas y 20 % de personas dijo que si existe excelentes medidas de seguridad para evitar la pérdida de información en preservación digital dentro de las diferentes instituciones.

9.- ¿Cree usted que la Preservación Digital tiene acceso a la información que se encuentra dentro de las diferentes instituciones?

SI ( )

NO ( )

Tabla 9-4: Porcentaje de la Pregunta 9

NO	SI
10	5
66,67%	33,33%

Realizado por: Marilú Torres, 2021

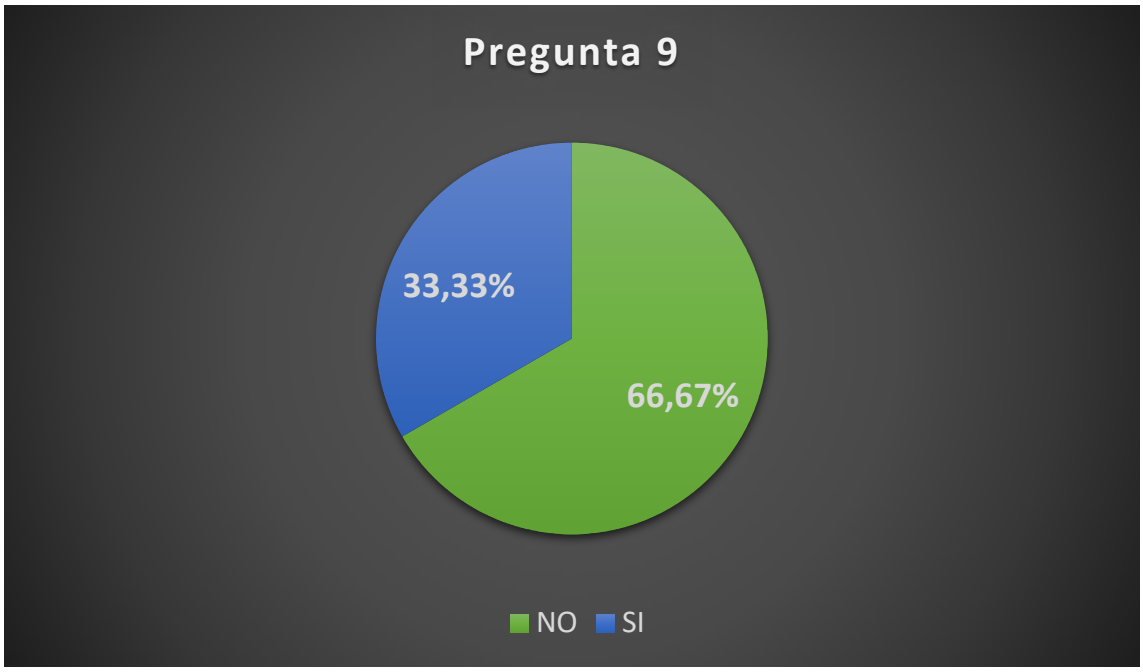


Gráfico 9-4: Porcentaje de la Novena Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 66,67 % de las personas encuestadas respondió que no recibe capacitaciones sobre el tema de preservación digital largo plazo dentro de sus instituciones, mientras que el 33,33 % de las personas encuestadas respondió que si recibe capacitaciones sobre el tema de preservación digital dentro de sus respectivas instituciones.

10.- Usted recibe capacitaciones sobre el tema de Preservación Digital a largo Plazo dentro de las Instituciones donde labora?

SI ( )
NO ( )

Tabla 10-4: Porcentaje de la Pregunta 10

NO	SI
13	2
86,67%	13,33%

Realizado por: Marilú Torres, 2021

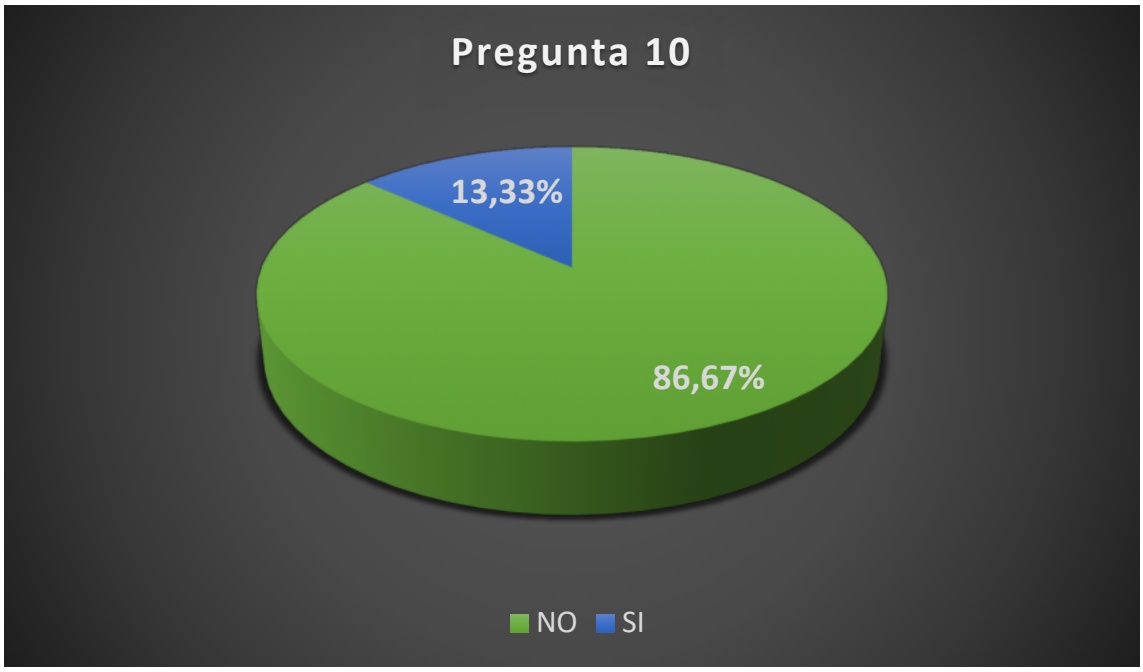


Gráfico 10-4: Porcentaje de la Décima Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 86,67 % de las personas encuestadas respondió que no se debe hacer preservación a largo plazo de manuscritos, libros, fotografías, audios, videos como patrimonio cultural, mientras que el 13,33 % que, si se debe hacer preservación a largo plazo de los manuscritos, libros, fotografías, audios que pueden ser patrimonio cultural.

Tabla 11-4: Tabla General de antes de aplicar el modelo de Preservación Digital

Preguntas	*Antes*					
	SI	*NO*	*MALA*	*BUENA*	*EXCELENTE*	*% de Aceptación*
1	4	11				26,67%
2	6	9				40%
3	3	12				20%
4	7	8				46,67%
5			5	6	4	40%
6	6	9				40%
7	4	11				26,67%
8			8	4	3	26,67%
9	5	10				33,33%
10	2	13				13,33%
						33,33%

Realizado por: Marilú Torres, 2021

4.2. Análisis de la situación Post-Implementación

1.- ¿Conoce usted si existen controles, normas para Archivar de manera correcta la Información en las instituciones?

SI ( )

NO ( )

Tabla 12-4: Porcentaje de la Pregunta 1

NO	SI
6	9
40%	60%

Realizado por: Marilú Torres, 2021

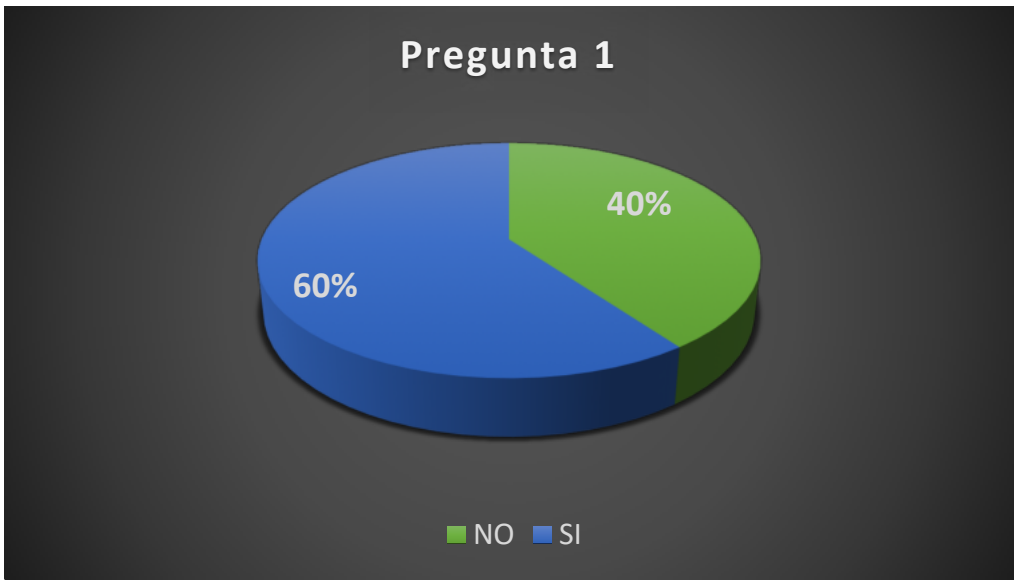


Gráfico 11-4: Porcentaje de la Segunda Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 40% de las personas encuestadas respondió que no existen controles para archivar la información dentro de las instituciones, mientras que el 60% manifestaron que si existen controles para archivar la información dentro de las diferentes instituciones.

2.- ¿Conoce Usted sobre la Preservación Digital a Largo Plazo?

SI ( )

NO ( )

Tabla 13-4: Porcentaje de la Pregunta 2

NO	SI
5	10
33,33%	66,67%

Realizado por: Marilú Torres, 2021

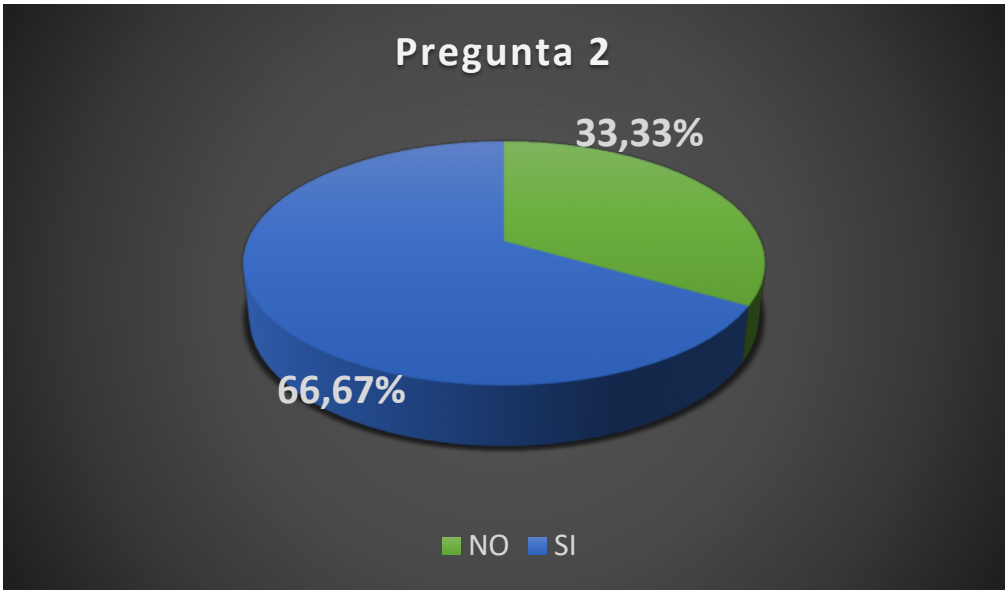


Gráfico 12-4: Porcentaje de la Segunda Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 33,33% de las personas encuestadas respondió que no sabe sobre el tema de preservación digital a largo dentro de las instituciones, mientras que el 66,67% manifestaron que si conocen sobre el tema de preservación digital dentro de las instituciones.

3.- ¿Sabe usted si la información es recopilada o preservada en las instituciones?

SI ( )

NO ( )

Tabla 14-4: Porcentaje de la Pregunta 3

NO	SI
7	8
46,67%	53,33%

Realizado por: Marilú Torres, 2021

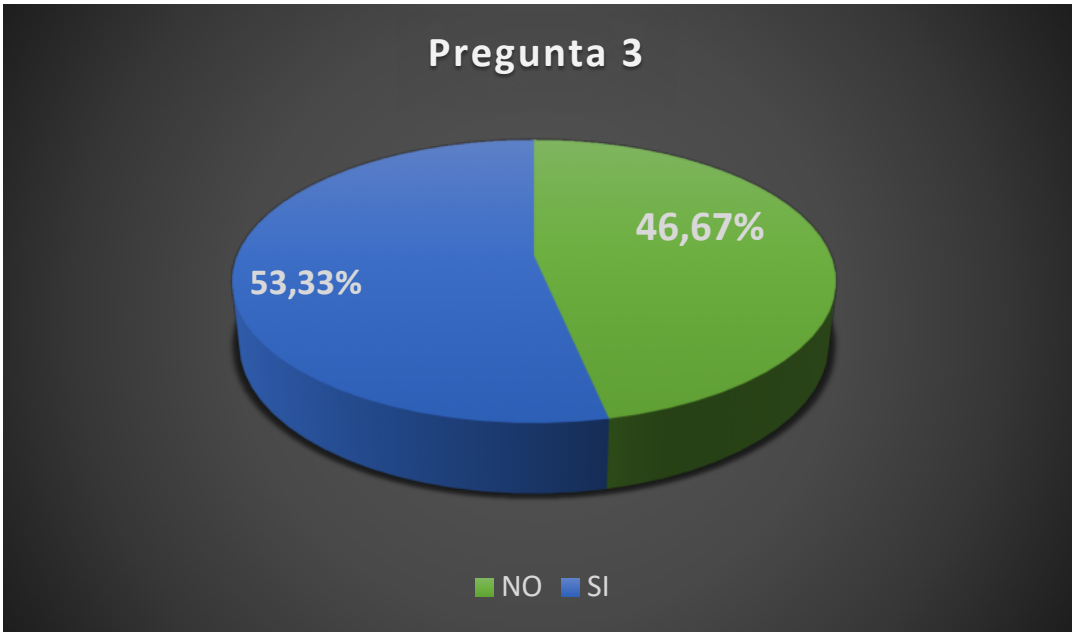


Gráfico 13-4: Porcentaje de la Tercera Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 46,67% de las personas encuestadas respondió que desconoce que las instituciones recopilen o preserven información, mientras que el 53,33% manifestaron que si saben que algunas instituciones recopilan o preservan información para que pueda ser accedida por diferentes personas o usuarios.

4.- ¿Sabe usted si se aplica preservación digital a la información en la actualidad?

SI ( )

NO ( )

Tabla 15-4: Porcentaje de la Pregunta 4

NO	SI
5	10
33,33%	66,67%

Realizado por: Marilú Torres, 2021

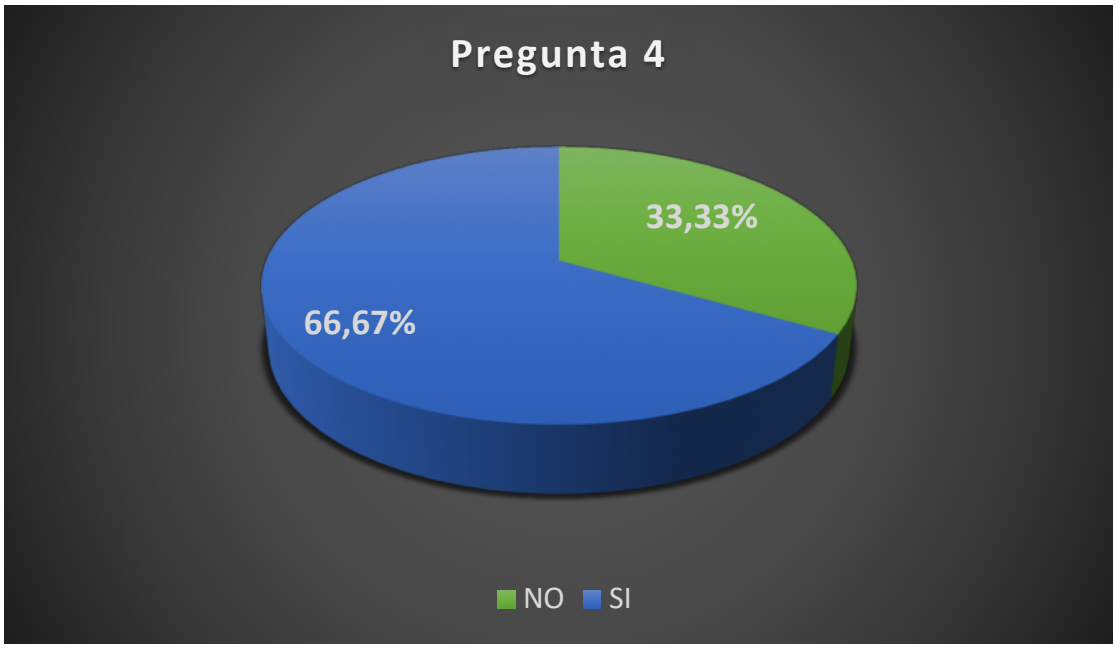


Gráfico 14-4: Porcentaje de la Cuarta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 33,33% de las personas encuestadas respondió que desconoce que se aplique preservación digital a la información en la actualidad dada por las

instituciones, mientras que el 66,67% manifestaron que si saben que se aplica preservación digital a la información en la actualidad dentro de las diferentes instituciones.

5.- ¿Cómo es la eficiencia en la atención del usuario (cliente) para obtener información?

Mala ( )

Buena ( )

Excelente ( )

Tabla 16-4: Porcentaje de la Pregunta 5

Mala	Buena	Excelente
3	7	5
20%	46,67%	33,33%

Realizado por: Marilú Torres, 2021

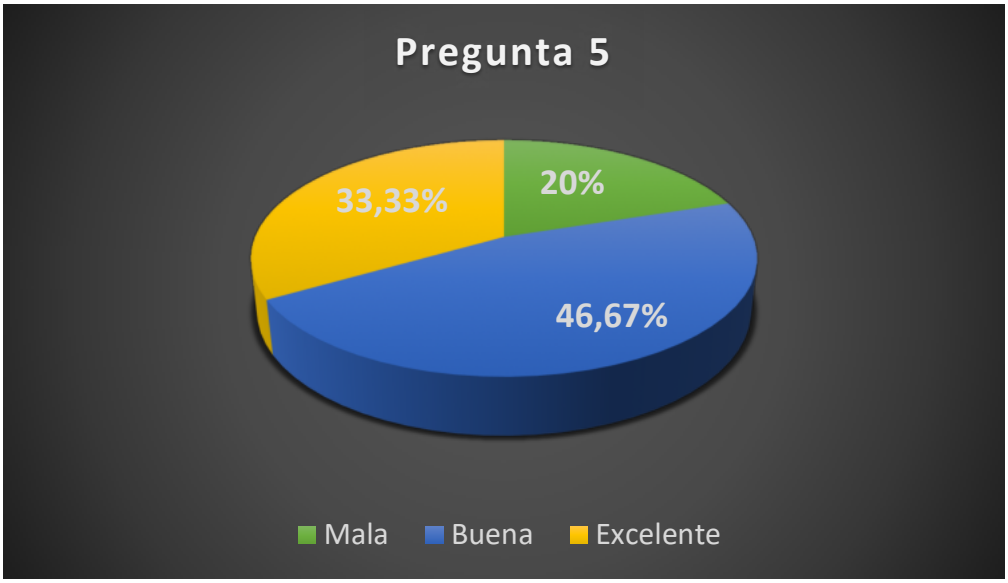


Gráfico 15-4: Porcentaje de la Quinta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 20 % de las personas encuestadas respondió que la atención a los usuarios (Clientes) es mala dentro de las diferentes instituciones, mientras que el 46,67% respondió que es buena y el 33,33% manifestaron que la atención a los usuarios (clientes) dentro de las diferentes instituciones es excelente.

6.- ¿Cree usted que la producción de Preservación Digital permite gestionar la información de manera adecuada dentro de las instituciones?

SI ( )
NO ( )

Tabla 17-4: Porcentaje de la Pregunta 6

NO	SI	
2	13	
13,33%	86,67%	

Realizado por: Marilú Torres, 2021

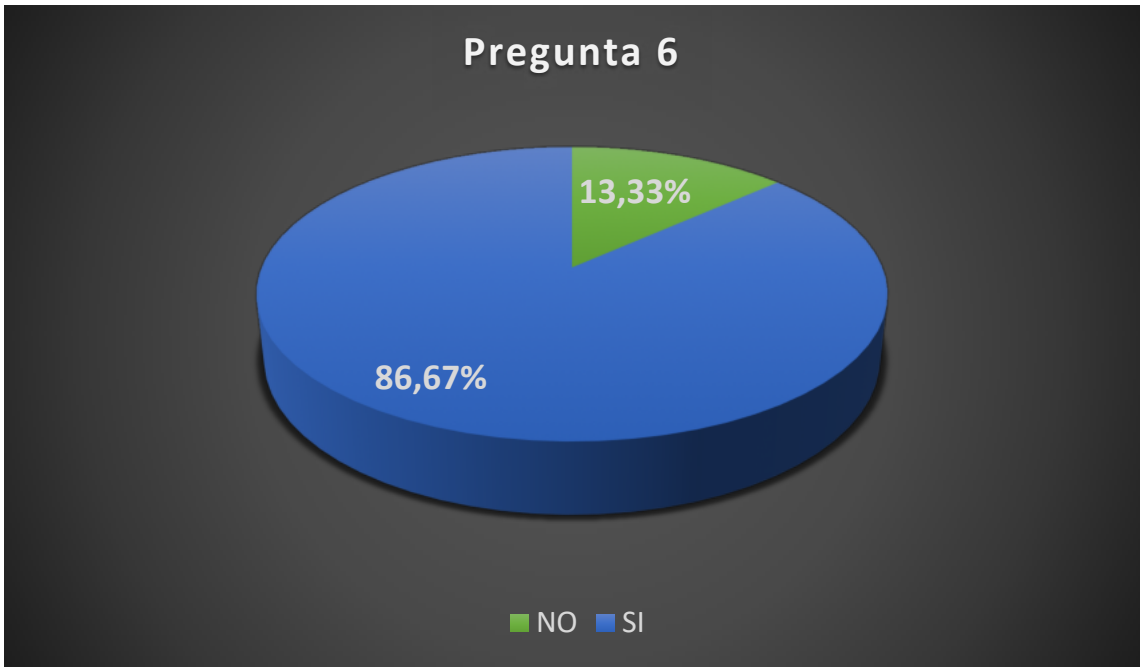


Gráfico 16-4: Porcentaje de la Sexta Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 13,33 % de las personas encuestadas respondió que la producción de preservación digital no permite gestionar de manera eficiente la información dentro de las instituciones mientras que el 86,67 % respondió que la producción de preservación digital permite gestionar de manera eficiente la información de las diferentes instituciones es buena.

7.- ¿Cree usted que las personas manejan la tecnología de manera correcta en la preservación digital dentro de las instituciones?

SI ( )

NO ( )

Tabla 18-4: Porcentaje de la Pregunta 7

NO	SI
7	8
46,67%	53,33%

Realizado por: Marilú Torres, 2021

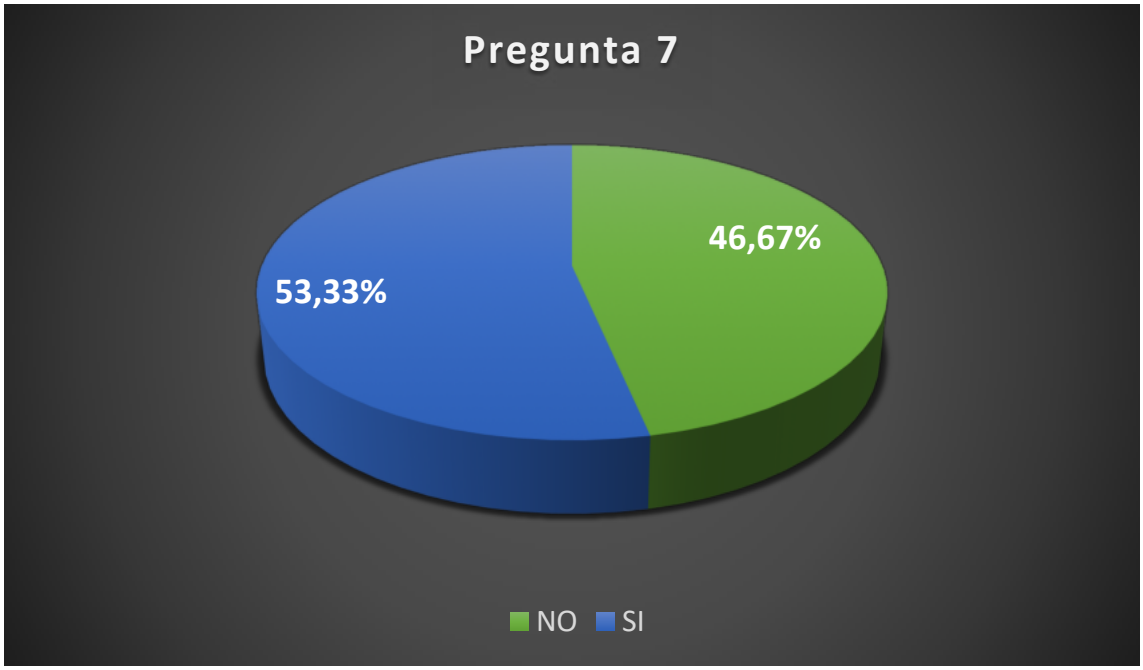


Gráfico 17-4: Porcentaje de la Séptima Pregunta

Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 46,67 % de las personas encuestadas respondió que no existen personas que manejen la tecnología de una manera correcta en la preservación digital dentro de las diferentes instituciones, mientras que el 53,337 % respondió que si existen personas que manejen la tecnología de una manera correcta en la preservación digital dentro de las diferentes instituciones.

8.- ¿Cree usted que las medidas de Seguridad para evitar la pérdida de la información en Preservación Digital son:

Mala ( )

Buena ( )

Excelente ( )

Tabla 19-4: Porcentaje de la Pregunta 8

Mala	Buena	Excelente
4	6	5
26,67%	40%	33,33%

Realizado por: Marilú Torres, 2021

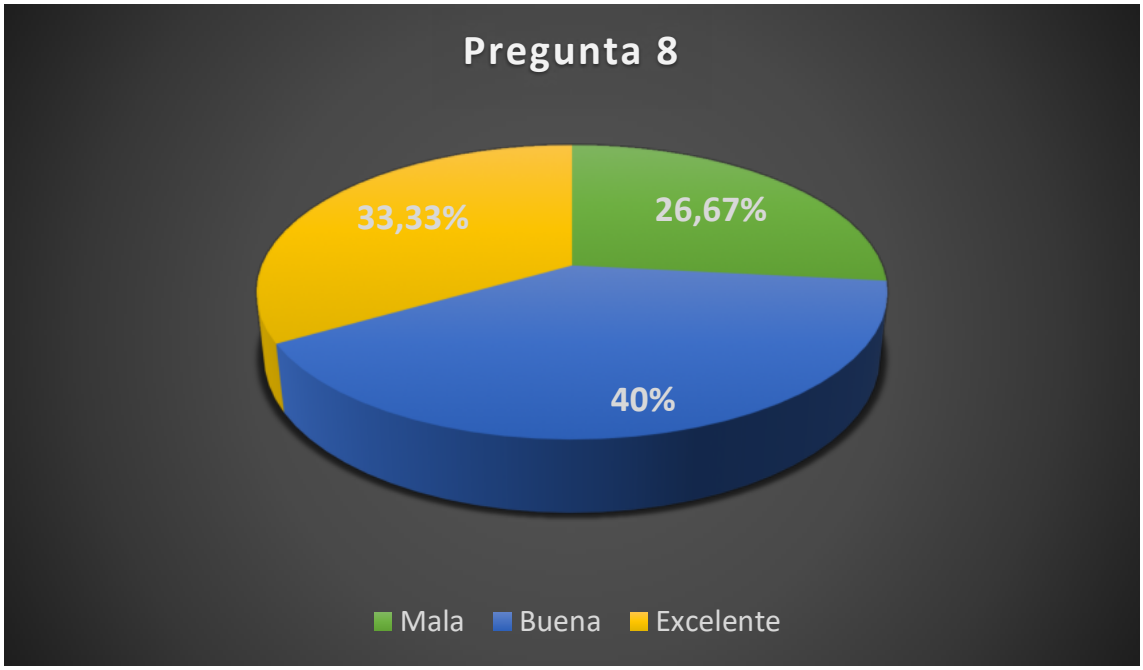


Gráfico 18-4: Porcentaje de la Octava Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 26,67 % de las personas encuestadas respondió que las medidas de Seguridad para evitar la pérdida de la información en Preservación Digital no existen dentro de las diferentes instituciones mientras que el 40 % respondió que son buenas y 33,33 % de personas dijo que si existe excelentes medidas de seguridad para evitar la pérdida de información en preservación digital dentro de las diferentes instituciones.

9.- ¿Cree usted que la Preservación Digital tiene acceso a la información que se encuentra dentro de las diferentes instituciones?

SI ( )

NO ( )

Tabla 20-4: Porcentaje de la Pregunta 9

NO	SI
3	12
20%	80%

Realizado por: Marilú Torres, 2021

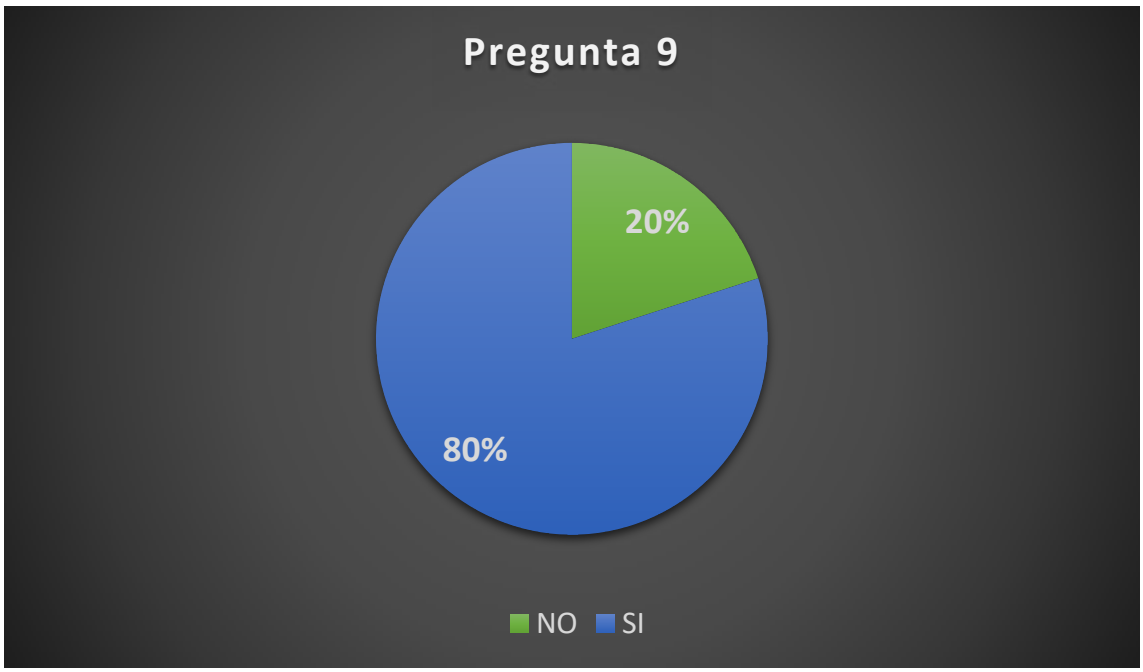


Gráfico 19-4: Porcentaje de la Novena Pregunta

Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 20% de las personas encuestadas respondió que la preservación digital no tiene acceso a toda la información que existe dentro de las diferentes, mientras que el 80% respondió que la preservación digital si tiene acceso a la información que se encuentran dentro de las diferentes instituciones.

10.- ¿Usted recibe capacitaciones sobre el tema de Preservación Digital a largo Plazo dentro de las Instituciones donde labora?

SI ( )
NO ( )

Tabla 21-4: Porcentaje de la Pregunta 10

NO	SI
4	11
26,67%	73,33%

Realizado por: Marilú Torres, 2021

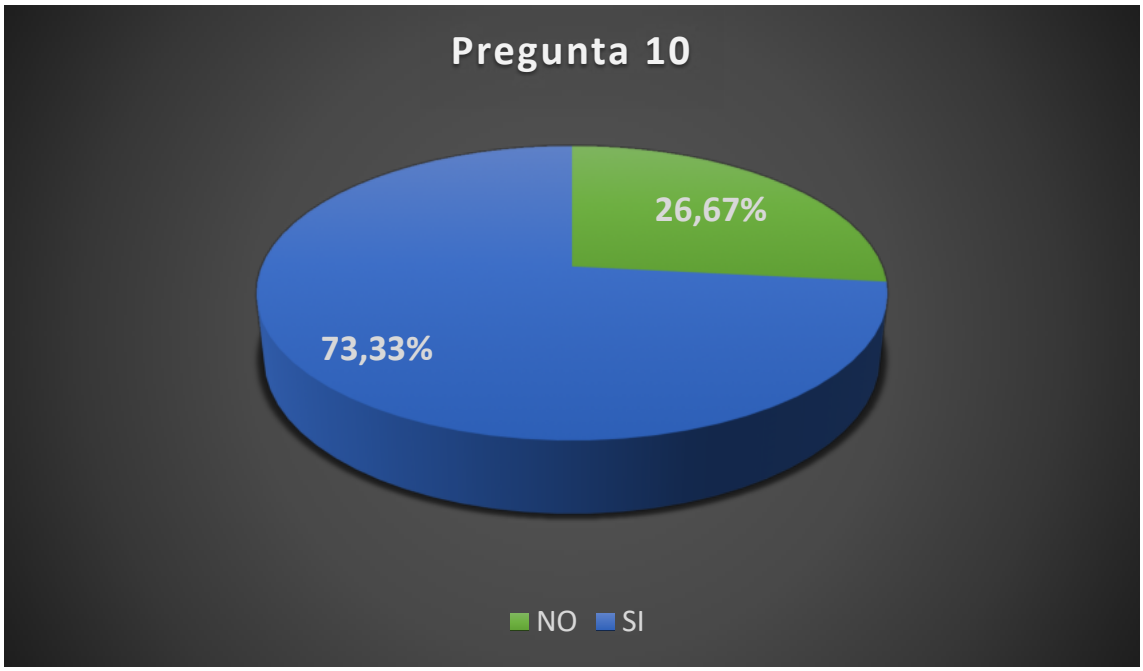


Gráfico 20-4: Porcentaje de la Décima Pregunta
Realizado por: Marilú Torres, 2021

En este gráfico se puede apreciar que el 26,67 % de las personas encuestadas respondió que no recibe capacitaciones sobre el tema de preservación digital largo plazo dentro de sus instituciones, mientras que el 73,33 % de las personas encuestadas respondió que si recibe capacitaciones sobre el tema de preservación digital dentro de sus respectivas instituciones.

Tabla 22-4: Tabla General de antes de la Post – Implementación

Preguntas	*Post-Implementación*					
	SI	***NO***	***MALA***	***BUENA***	***EXCELENTE***	***% de Aceptación***
1	9	6				60%
2	10	5				66,67%
3	8	7				53,33%
4	10	5				66,67%
5			3	7	5	46,67%
6	13	2				86,67%
7	8	7				53,33%
8			4	6	5	40%
9	13	3				80%
10	11	4				73,33%
						62,67%

Realizado por: Marilú Torres, 2021

Tabla 2-4: Comparación de la Tabla Pre-Implementación vs Post-Implementación

Preguntas	*Antes*	*Post-Implementación*
1	26,67%	60%
2	40%	66,67%
3	20%	53,33%
4	46,67%	66,67%
5	40%	46,67%
6	40%	86,67%
7	26,67%	53,33%
8	26,67%	40%
9	33,33%	80%
10	13,33%	73,33%

Realizado por: Marilú Torres, 2021

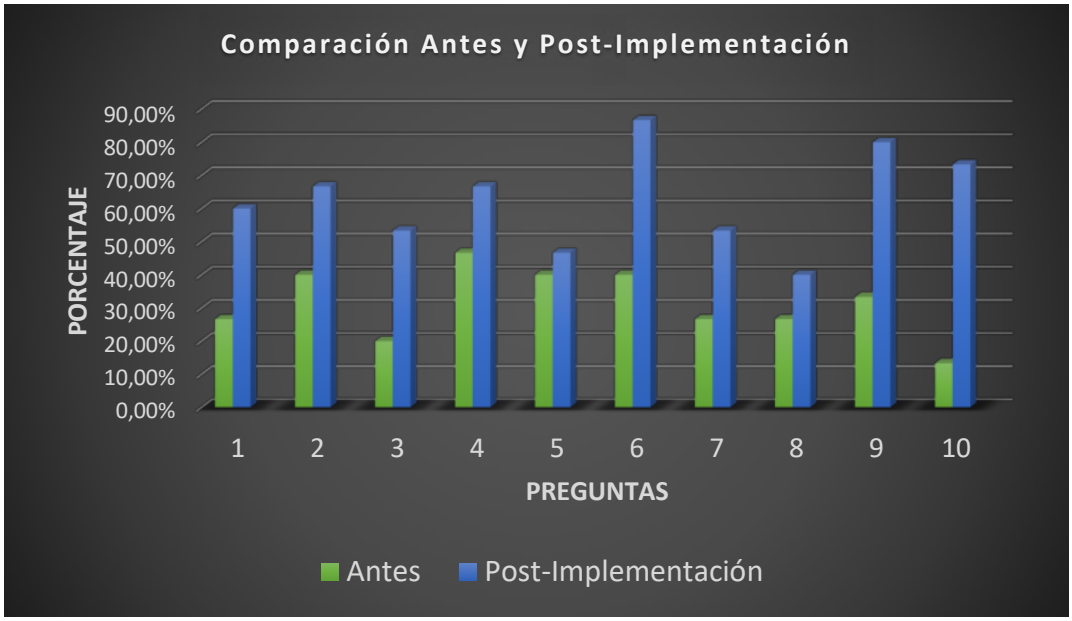


Gráfico 21-4: Comparación de Porcentajes Antes y Post-Implementación
Realizado por: Marilú Torres, 2021

Tabla 24-4: Comparación de la Tabla (Pre vs Post) Implementación valores Finales

Antes	Post-Implementación
33,33%	**62,67%**

Realizado por: Marilú Torres, 2021

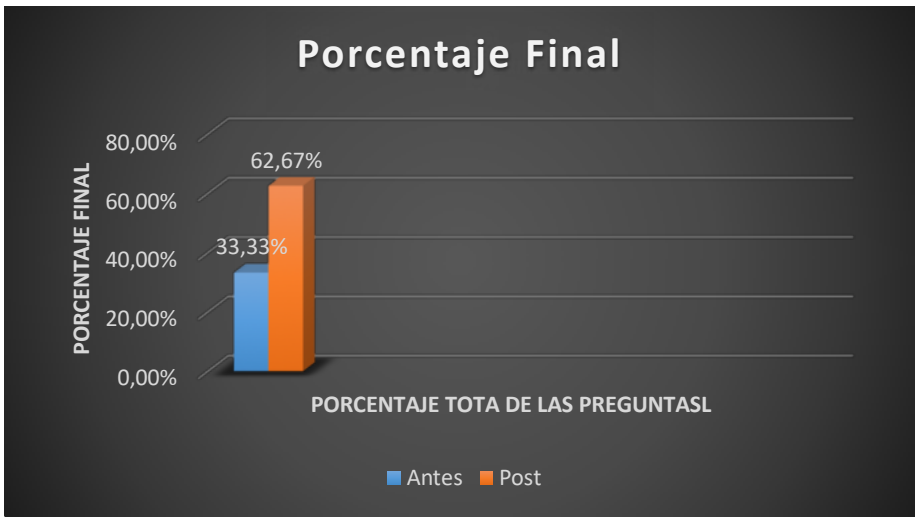


Gráfico 22-4: Comparación de Porcentajes Finales Antes y Post-Implementación
Realizado por: Marilú Torres, 2021

En la gráfica se puede observar los resultados de la comparación de porcentajes finales de antes y Post-Implementación, que está formado por 10 preguntas, obteniendo así que el 33.33% de las personas encuestadas indican un nivel de desconocimiento sobre el tema de Preservación Digital a Largo Plazo que existen dentro de las diferentes instituciones, seguido del 62,67%% de nivel de importancia al realizar la encuesta después de haber aplicado el modelo de preservación lo cual nos permite conocer que después de realizar diferentes capacitaciones sobre el tema los parámetros mejoraron con respecto al primer análisis.

4.3. Comprobación de Hipótesis

La prueba paramétrica t para dos muestras emparejadas es una prueba de hipótesis que intenta hacer una afirmación sobre las medias.

Más específicamente, una prueba t usa información de muestra para evaluar qué tan plausible es que la diferencia μ_1- μ_2 sea igual a cero. La prueba tiene dos hipótesis que no se superponen, la hipótesis nula y la hipótesis alternativa. La hipótesis nula es un enunciado sobre el parámetro de población que indica que no hay efecto, y la hipótesis alternativa es la hipótesis complementaria a la hipótesis nula.

Se aplica cuando la población estudiada sigue una distribución normal pero el tamaño de la muestra es demasiado pequeño como para que el estadístico en el que está basada la inferencia esté normalmente distribuido, utilizándose una estimación de la desviación típica en lugar del valor real.

4.4. Planteamiento de la Hipótesis

Hipótesis de investigación Hi: La implementación de un modelo basado en la norma internacional ISO/IEC 27001 permite obtener la integridad de documentos informáticos**.**

Hipótesis de Nula H_0: La implementación de un modelo basado en la norma internacional ISO/IEC 27001 no permite obtener la integridad de documentos informáticos.

1. H_o: $\mu_{\bar{d}} = 0$

Hipótesis Alternativa H_1: La implementación de un modelo basado en la norma internacional ISO/IEC 27001 permite obtener la integridad de documentos informáticos.

2. H1: $\mu_{\bar{d}} \neq 0$

Donde$\mu_{\bar{d}}$ es la media de las medidas.

4.3.2. Nivel de Significancia

Se debe elegir un nivel de significancia para la prueba que permite analizar los resultados de la prueba son estadísticamente significativos y también determina la probabilidad de error que es inherente a la prueba.

Para nuestra investigación se establece un nivel de significancia (denotado como α o alfa) de 0.05. Un nivel de significancia de 0.05 indica un riesgo de 5% de concluir que existe una diferencia cuando no hay una diferencia real.

$$\alpha = 0.05$$

4.3.3. Prueba Estadística

En función de los datos obtenidos utilizamos la distribución T de Student, donde se establece que:

$$t_c = \frac{\bar{d}}{\frac{S_d}{\sqrt{n}}}$$

$$S_d = \sqrt{\frac{\sum_{i=1}^{n}(d - \bar{d})^2}{n-1}}$$

Donde:

t_c = valor estadístico del procedimiento calculado.

$\bar{d}$ = Valor promedio o media aritmética de las diferencias entre los momentos antes y después.

S_d = desviación estándar de las diferencias entre los momentos antes y después.

n = tamaño de la muestra.

4.3.4. *Regla de Decisiones*

Caso 1.

$$t_c > t_\alpha, rechaza\ la\ hipotesis\ nula\ H_0$$

Caso 2.

$$Valor\ p < \alpha, se\ rechaza\ la\ hipotesis\ nula\ H_0$$

4.3.5. Conclusiones

La data fue evaluada en la herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras emparejadas, de Microsoft Excel.

Normalidad

Para la prueba de Normalidad en la que se debe aceptar la hipótesis nula y se consideran todas las categorías de riesgos ponderadas según la siguiente tabla:

Tabla 27-4: Datos Iniciales y de Post-Implementación

ITEM	AMENAZAS	Valoración Inicial	Valoración Post-Implementación
1	Mecanismos de Autenticación (Contraseñas)	1,68	0,12
2	Acceso no autorizado a la información o datos	1,2	1,8
3	Herramientas de Seguridad Implementadas	2,88	0,84
4	Errores de usuarios y operadores	1,44	0,60

Realizado por: Marilú Torres, 2021

Resultados de la prueba t Student

	Variable 1	*Variable 2*
Media	3,3140	0,606
Varianza	0,3632	0,43133
Observaciones	5,0000	5
Coeficiente de correlación de Pearson	-0,6120	
Diferencia hipotética de las medias	0,0000	
Grados de libertad	4,0000	
Estadístico t	5,3543	
P(T<=t) una cola	0,0029	
Valor crítico de t (una cola)	2,1318	
P(T<=t) dos colas	0,005869	
Valor crítico de t (dos colas)	2,7764	

Fuente: Herramienta Análisis de Datos, con la función Prueba t para medias de dos muestras emparejadas.

En promedio de los riesgos de amenazas inicial es 3,3140 mayor que los riesgos de amenaza post implementación igual 0,606, hay una diferencia significativa

El valor de P, que es el nivel de significancia cuyo valor es 0,005869, es menor que el valor determinado para α = 0,05 por lo que nos lleva a rechazar la hipótesis nula H0 y aceptar la alternativa H1.

Con esto concluimos que la diferencia de las medias de los riesgos obtenidos con amenaza inicial y post-Implementación, son significativamente diferentes con un nivel de confianza del 95%.

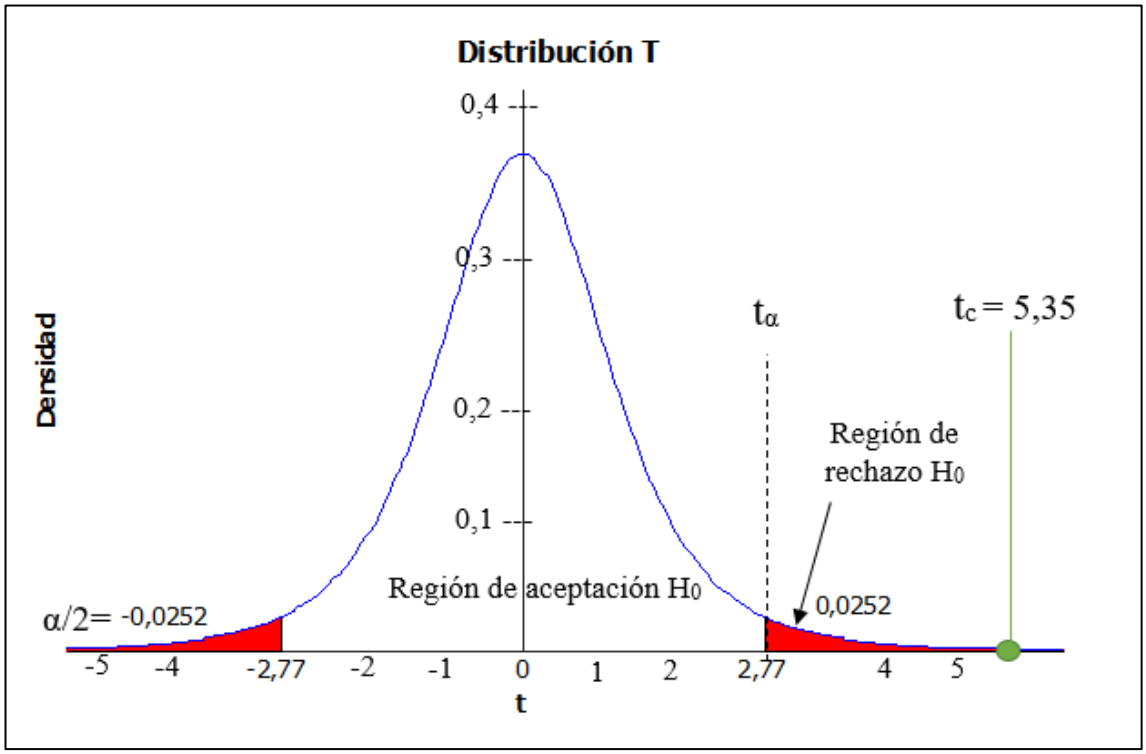


Gráfico 23-4: Gráfico de distribución de zona de rechazo y aceptación de la hipótesis.
Realizado por: Marilú Torres, 2021

El valor del estadístico t_c está en la zona de rechazo, por lo que se rechaza la hipótesis nula. Por tanto, existe evidencia estadística de que la implementación de un modelo basado en la norma internacional ISO/IEC 27001 permite obtener la integridad de documentos informáticos.

CONCLUSIONES

- La conclusión más importante que se puede mencionar es que se logró analizar la seguridad informática e información utilizando la norma ISO/IEC 27001 que permite diseñar un modelo para la verificación de integridad de documentos informáticos.

- Se realizó el análisis de las leyes, reglamentos y estatutos vigentes relacionadas con preservación de documentos informáticos.

- Se estudiaron los modelos de preservación digital documental que permiten asegurar los datos a largo plazo tales como: PREDECI, OAIS, PREMIS, DAMM, los cuales fueron analizados y comparados mediante la entrevista realizada.

- Dado el caso de estudio, el modelo de preservación digital que tuvo mayor puntaje y que se propone implementar es el modelo PREDECI, el que cumple con todos los requerimientos funcionales de las directrices de la UNESCO, con los parámetros de la Norma ISO/IEC 27001 y con los criterios de NESTOR logrando garantizar la información de los objetos digitales.

- El modelo de Preservación digital estuvo evaluado por los criterios de NESTOR el cual permitió obtener resultados de cada uno de los criterios establecidos y se pudo obtener el nivel de integridad de los datos (Información).

- En la comparación de resultados Antes y Post Implementación se pudo concluir que en la primera fase se obtuvo un resultado del 33,33% que las personas desconocen sobre el tema de preservación digital y luego de la implementación se obtuvo 62,67% teniendo un nivel favorable de aceptación, validación de los resultados sobre el tema de preservación digital a largo plazo.

- El resultado de la encuesta aplicada a los usuarios evidencia que la prestación de servicios por parte de la institución no es óptima dado que la mayoría desconoce sobre el tema de preservación digital y que falta muchas capacitaciones que enfatice en el tema de preservación digital y además contribuye a la modernización del sistema.

- Con el respectivo análisis realizado del modelo de preservación digital PREDECI se aplicó todas las seis entidades funcionales, que son Ingestas, Área de Almacenamiento, Gestión de Datos, Administración, Plan de Preservación y Acceso, en el desarrollo de la investigación de Preservación de Documentos Digitales.

RECOMENDACIONES

- Se debe recopilar toda la información disponible de fuentes bibliográficos, libros, tesis, artículos científicos actualizados porque referente a este tema esta información puede quedar obsoleta con el pasar de los tiempos en la búsqueda de beneficios.

- Se recomienda hacer capacitaciones con programas y estrategias de manera periódicas a los usuarios (Clientes) y personal de las instituciones que brindan este servicio de preservación digital.

- Para hacer un análisis de manera específica para los modelos de preservación digital se debe tomar en cuenta todos los parámetros que ayuden a tomar la mejor decisión y estos deben estar acorde con el avance tecnológico.

- Los profesionales en el área de preservación digital deben continuar con procesos de actualización y formación acorde a los cambios tecnológicos, legales, etc.

BIBLIOGRAFÍA

[1] Anne, Thurston. (Septiembre de 2012). Digitization and Prevencion : Global Opportunites and Cultural Challenges. International conference on permanent accesse to digital documentary heritage (págs. 31-47). Vancouver, UBC. Canada: Luciana Duranti and Elizabeth.

[2] Álvarez-Wong, B. I. (2017). Los repositorios digitales para la conservación. Un acercamiento a la preservación digital a largo plazo. 48(2), 15-22. Obtenido de http://www.redalyc.org/pdf/1814/181454540003.pdf

[3] Alvear Guerrero, Y. del S., & Abelló Hernández, L. M. (2019). Estado del Arte de la Preservación de Documentos Digitales en los Países de México, Colombia, Brasil y Argentina: 2006—2016 [Universidad de la Salle]. Facultad de Ciencias Económicas y Sociales. Maestría en Gestión Documental Administración de Archivos. Bogotá, Colombia. https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1049&context=maest_gestion_documental

Aquino. (22 de Noviembre de 2016). Retos de la preservación digital. Obtenido de Retos de la preservación digital.: http://www.infotecarios.com/

[4] Ausay Espinoza, M. F., & Valle Padilla, W. E. (2019). Aplicación de un Modelo de Preservación Digital para Garantizar la Integridad al Largo Plazo de la Información de Archivos del GADM-RIOBAMBA [Universidad Nacional de Chimborazo]. Facultad de Ingeniería de Sistemas e Informática. Riobamba, Ecuador. http://dspace.unach.edu.ec/handle/51000/5577

[5] Bermúdez Molina, K. G., & Bailón Sánchez, E. R. (2015). Análisis en Seguridad Informática y Seguridad de la Información Basado en la Norma ISO/IEC 27001- Sistema de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financieros [Universidad Politécnica Salesiana sede Guayaquil]. Ingeniería en Sistemas. Guayaquil, Ecuador. https://dspace.ups.edu.ec/bitstream/123456789/10372/1/UPS-GT001514.pdf**[6]** Boté Vericad, J. J. (2012). Propuesta de un Modelo de Preservación Digital para Pequeñas y Medianas Instituciones Sanitarias. [Universidad de Barcelona]. Barcelona, España. https://www.tdx.cat/bitstream/handle/10803/96254/JJBV_TESIS.pdf?sequence=1&isAllowed=y

[7] Castillo Segura, C. C. (s. f.). Fundamentos de Preservación Digital a Largo Plazo [Archivo General de la Nación de Colombia]. Bogotá, Colombia.

https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/FundamentosPreservacionLargoPlazo.pdf

[8] Cerón Romo, F. A., Marín Bohórquez, L. F., & Gómez Martínez, J. A. (2017). Repositorio Digital de Artículo, Tesis, Libros, Congresos y otros Documentos sobre el Área de Proyectos [Universidad de San Buenaventura Colombia]. Facultad de Ingeniería. Especialización en Gestión Integral de Proyectos. Santiago de Cali, Colombia. http://bibliotecadigital.usbcali.edu.co:8080/bitstream/10819/5492/1/Repositorio%20_digital_%20art%C3%ADculos_%20proyectos_ceron_2017.pdf

[9] Giménez, V. C. (2014). Criterios ISO para la preservación digital de los documentos de archivo. Universitat Politècnica de València, España, 135-150.

[10] Giusti, M. (2015). Preservación Digital. Preservación Digital, Universidad Complutense de Madrid. http://sedici.unlp.edu.ar/bitstream/handle/10915/44406/Preservaci%C3%B3n_digital._Metadatos_y_preservaci%C3%B3n_-_Clase_dictada_por_Marisa_De_Giusti__69_diap._.pdf?sequence=6&isAllowed=y

[11] Giusti, M. d. (2014). Una metodología de evaluación de repositorios na digitales para asegurar la preservación en el tiempo y el acceso a los contenid.

[12] Guachi Aucapiña, T. V. (2012). Norma de Seguridad Informática ISO 27001 para Mejorar la Confidencialidad, Integridad y Disponibilidad de los Sistemas de Información y Comunicación en el Departamento de Sistemas de la Cooperativa de Ahorro y Crédito SAN FRANCISCO LTDA. [Universidad Técnica de Ambato]. Facultad de Ingeniería en Sistemas, Eléctrica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos. Ambato, Tungurahua, Ecuador https://repositorio.uta.edu.ec/bitstream/123456789/2361/1/Tesis_t715si.pdf

[13] Guarnizo Arias, J. E., & Prieto Sarmiento, E. J. (2016). Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para la Empresa AGILITY S.A.S [Universidad Distrital Francisco Jode de Caldas]. Facultad de Tecnología, Carrera de Telemática. Bogotá, Colombia. https://repository.udistrital.edu.co/bitstream/handle/11349/4709/PrietoSarmientoEdwardJonathan2019.pdf?sequence=1&isAllowed=y

[14] Leíja Román, D. A. (2017). Preservación Digital Distribuida y la Colaboración Interinstitucional: Modelo de Preservación Digital para Documentos con Fines de Investigación en Universidades de México [Universidad de Barcelona]. Doctorado en Información del Conocimiento. Barcelona, España. https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1059&context=maest_gestion_documental

[15] Molina Fernando y Rodriguez Glen . (2017). Model for digital evidence preservation in criminal research institutions - PREDECI. International Journal of Electronic Security and Digital Forensics, 150

[16] NESTOR, F. a. (2009). Catalogue of Criteria for Truested Digital Repositories Version 2. nestor Working Group Truested Repositories - Certification.

[17] Nacipucha Cumbe, J. C. (2019). Análisis y Diseño para un Modelo de Gestión de Seguridad de la Información Basados en Normas ISO/IEC 27001:2013 para la Empresa ARTEHOGAR en la Ciudad de Guayaquil. Universidad de Guayaquil. Facultad de Ciencias Administrativas. Carrera de Ingeniería en Sistemas. Guayaquil, Ecuador. http://repositorio.ug.edu.ec/bitstream/redug/44410/1/Tesis%20Nacipucha%20%2802%2009%29%20impresion.pdf

[18] Peña, B. (2015). Propuesta para el Diseño de un Repositorio Digital para el Centro de Información y Documentación «willy-ossott» de la Facultad de Arquitectura y Urbanismo. Universidad Central de Venezuela. Facultad de Humanidades y Educación. Escuela de Bibliotecología y Archivología. http://saber.ucv.ve/bitstream/123456789/16920/1/Tesis%20Beatriz%20Pe%C3%B1a.pdf

[19] Pilco Pilco, R. G. (2015). Análisis de los Modelos de Preservación Digital en Software Libre para la Preservación de la Producción Académica de la Carrera de Ingeniería en Sistemas y Computación [Universidad Nacional de Chimborazo]. Facultad de Ingeniería. Carrera de Ingeniería en Sistemas y Computación. Riobamba, Ecuador. http://dspace.unach.edu.ec/bitstream/51000/467/1/UNACH-EC-IINDUST-2015-0012.pdf

[20] Plan de Preservación Digital. (2020). [Ministerio de Educación Nacional]. https://www.mineducacion.gov.co/1759/articles-392395_PLanes2020__02.pdf

[21] Remolina Becerra, L. C. (2019). Diseño de un Modelo de Seguridad Informática a una Empresa en su Sistema de Monitoreo del Área de tecnología [Universidad Cooperativa de Colombia]. Facultad de Ingeniería. Bogotá, Colombia. https://repository.ucc.edu.co/bitstream/20.500.12494/18082/1/2020_Diseño_modelo_seguridad.pdf

[22] Sánchez Salazar, J. (2019). Estrategia para la Preservación de Documentos Digitales en el Archivo de la Secretaría de la Junta Directiva del Banco de la Republica de Colombia [Universidad de la Salle]. Facultad de Ciencias Económicas y Sociales. Maestría en Gestión Documental y Administración de Archivos. Bogotá, Colombia. https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=1059&context=maest_gestion_documental

[23] Térmens, M. (2010). Perspectivas para la sostenibilidad y la preservación de los repositorios institucionales. Presentación. 4as Jornadas OS-Repositorios. Barcelona**[24]** UNESCO. (2003). Directrices para la Preservacion del Patrimonio Digita. National Library of Australia, 12. Obtenido de http://unesdoc.unesco.org/images/0013/001300/130071s.pdf.

[25] UNESCO. (2017). @UNESCO. Obtenido de Programa Memoria del Mundo (MoW): Preservando el patrimonio documental: http://www.unesco.org/new/es/santiago/communication-information/memory-of-the-world-programme-preservation-of-documentary-heritage/

Voutssas, J. (2010). Preservación documental digital. Centro Universitario de Investigaciones Bibliotecológicas de la UNAM, 127-155.

[26] Webb, C. (2003). DIRECTRICES PARA LA PRESERVACIÓN DEL PATRIMONIO DIGITAL. Biblioteca Nacional de Australia.

ANEXO

Anexo 1 A: MODELOS DE LA ENCUESTA

	ESCUELA SUPERIOR POLITECNICA DE CHIMBORAZO			
	ENCUESTA SOBRE PRESERVACION DIGITAL			
Ítems	***Pregunta***	***Respuesta***		
1	¿Conoce usted si existen controles, normas para Archivar de manera correcta la Información en las instituciones?	SI ( )	NO ( )	
2	¿Conoce Usted sobre la Preservación Digital a Largo Plazo?	SI ( )	NO ( )	
3	Sabe usted si la información es recopilada o preservada en las instituciones?	SI ( )	NO ( )	
4	¿Sabe usted si se aplica preservación digital a la información en la actualidad?	SI ( )	NO ( )	
5	¿Cómo es la eficiencia en la atención del usuario (cliente) para obtener información?	Mala ( )	Buena ( )	Excelente ( )
6	¿Cree usted que la producción de Preservación Digital permite gestionar la información de manera adecuada dentro de las instituciones?	SI ( )	NO ( )	
7	¿Cree usted que las personas manejan la tecnología de manera correcta en la preservación digital dentro de las instituciones?	SI ( )	NO ( )	
8	¿Cree usted que las medidas de Seguridad para evitar la pérdida de la información en Preservación Digital son:	Mala ( )	Buena ( )	Excelente ( )
9	¿Cree usted que la Preservación Digital tiene acceso a la información que se encuentra dentro de las diferentes instituciones?	SI ( )	NO ( )	
10	Usted recibe capacitaciones sobre el tema de Preservación Digital a largo Plazo dentro de las Instituciones donde labora?	SI ( )	NO ( )	

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

DBRAI

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: *17 / 11 / 2021*

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: *Marilú del Cisne Torres Romero*
INFORMACIÓN INSTITUCIONAL
Instituto de Posgrado y Educación Continua
Título a optar: *Magíster en Seguridad Telemática*
f. Analista de Biblioteca responsable: *Lic. Luis Caminos Vargas Mgs.*

LUIS ALBERTO CAMINOS VARGAS

Firmado digitalmente por LUIS ALBERTO CAMINOS VARGAS
DN: cn=LUIS ALBERTO CAMINOS VARGAS c=EC l=RIOBAMBA
Motivo: Soy el autor de este documento
Ubicación:
Fecha: 2021-11-17 17:37-05:00

UNIDAD DE PROCESOS TÉCNICOS DBRAI ESPOCH